

E-Book made by [Jagson](#) - Hackforums

Introduction

So you want to learn how you can RAT any kind of person you want? I will tell you something, you can! If you are really motivated to learn how you can RAT, then you will and I will help you on this path.

I'm already over a year into ratting. I'm not the kind of person who steals money or passwords but I have a good amount of knowledge about this scene and I want to explain you some programs, crypter and tools!

I will show you what you can do with your slaves for example earn money, make fun with them, make videos and much more. All this you will find in my Ebook.

I will introduce you in in some RATS that are actually one of the best on the market and I will introduce you in Cammy. If you don't know what Cammy is, then wait a little bit, because I will describe it later.

What are RATs exactly?

RATs is just a short form for **Remote Administrative Tools**, some people call it **Remote Administrative Trojan** but I would not recommend this.

A RAT is a program with that you can make a connection to another PC and through that, you can control the computer. You can watch their screen or webcam, or you can recover passwords and record the keyboard (Called Keylogger) and many other things. Normally it will be used from big companies for remote maintenance or similar, but you can use it for your own purposes.

The most RATs are just made for Windows. The Darkcomet RAT for example, can still be used for Windows 8 although there will be no new upgrade anymore. I would not recommend to focus a MAC, because it's almost impossible to rat a MAC without any permission from the owner of the PC.

Useful Links:

Darkcomet Download, Every Version: <http://www.hackforums.net/showthread.php?tid=2632776>

Cammy Download: Thread link: <http://www.ic0de.org/showthread.php?9205-Cammy-2-0>
(You have to register)

Direct Download: <http://ge.tt/9DFCJ2p/v/0>

All RATS **SHOULD** have those features as a basic:

- Screen/Desktop capture or image control
- Webcam capture
- File management (download/upload/execute/etc)
- Shell control
- Computer control (power off/power on/log off/etc)
- Registry management (query/add/delete/modify)
- Record victims Keystrokes (Keylogger)
- DDoS
- Block mouse and keyboard
- Change your desktop wallpaper
- Download, upload, delete, and rename files
- Drop viruses and worms
- Edit Registry
- Format drives
- Grab passwords
- Hijack homepage
- Hide desktop icons, taskbar and files
- Log keystrokes, keystroke capture software
- Open/Close CD-ROM tray
- Overload the RAM/ROM drive
- Print text
- Play sounds
- Randomly move and click mouse
- Record sound with a connected microphone
- Record video with a connected webcam
- Shut-down, Restart, Log-Off, Shutdown monitor
- View screen
- View, kill, and start tasks in task manager

What is Cammy?

Cammy is almost the same as a RAT like Darkcomet, but it is specialized on looking on the Desktop screen and the Webcam. It is really fast, faster than the most RATs, so if you want to record a Webcam, I would recommend this program. But with the good benefits it has, it also has a disbenefit, its very unstable, but I know plenty tricks how you can make it stable, so you don't have to be scared! I will explain it to you later.

Cammy is also an open source project, so if you have some programming skills, you can develop the program for your own purpose.

Dangers

Before I really start to explain how you can use those products I want to say a few words about the dangers when you are into hacking. Rating is illegal if you do it without any permission from the owner of the computer. If you get caught, then you have a problem, a big problem! There are several methods how you can save your ass, I will explain that later, but be sure that you really want to do this. If you can't handle the consequence, than you should not do this. But if you follow my instructions then you shouldn't get caught, so rate my tips as gold, it's very important.

What do you need?

You just need some things for your purpose, some are free and some not. Many things you need you can get for free on forums, like Hackforums.net, and some things you should better buy, I will tell you which programs you should buy, don't worry.

What do you need?

1. A Remote Administrative Tools (RAT)
 - a. Darkcomet – It's for free, but it will not be upgraded anymore because the coder dont want to do it anymore
 - b. Blackshades – It cost you some Money, but it's actually one of the best on the market.
 - c. Imminent Monitor – It's my favorite RAT, it's really fast and it makes Cammy unimportant for the future. Unfortunately you shouldn't use it to download files from a Slaves PC, because you cant mark a group of file which you want to download it. You should wait until Version 3, it will come out soon, then you can download plenty of file at once.

2. A Crypter – It will make your file fully undetected, so Anti Viruses can't detect and destroy it before it can be run on the victims Computer. **I highly recommend to buy a good one.**
 - a. Codelux Crypter - <http://www.hackforums.net/showthread.php?tid=3500882> – I highly recommend this Crypter, its very stable and almost **ALWAYS** FUD* (Fully Undetected), the coder brings almost every day an Update
 - b. Infinite Crypter - <http://www.hackforums.net/showthread.php?tid=3051402> – It's very stable, but not always FUD* because of the amount of Users it has.
 - c. Dark Eye Crypter V2 - <http://www.hackforums.net/showthread.php?tid=3181490> – it's one of the best Crypter, its expensive but definitely worth it, almost always FUD.

3. A VPN (Virtual Private Network) – It will help you not to get caught while you are ratting. It will hide your real IP from the victim. I also recommend to buy a VPN, I would recommend a VPN in the East, like Russia.

- a. NVPN - <http://nvpn.net> – I would recommend this one, it's by far one of the best, its cheap, it has many country locations which you can choose and the best, they don't save logs. If you buy a VPN from them, choose the function "Dynamic IP", it will be better for our use and makes your whole actions safer. With this function you have always different IP addresses and not just a single one, it will cost a little bit more, but it's not very much.

Advertisement



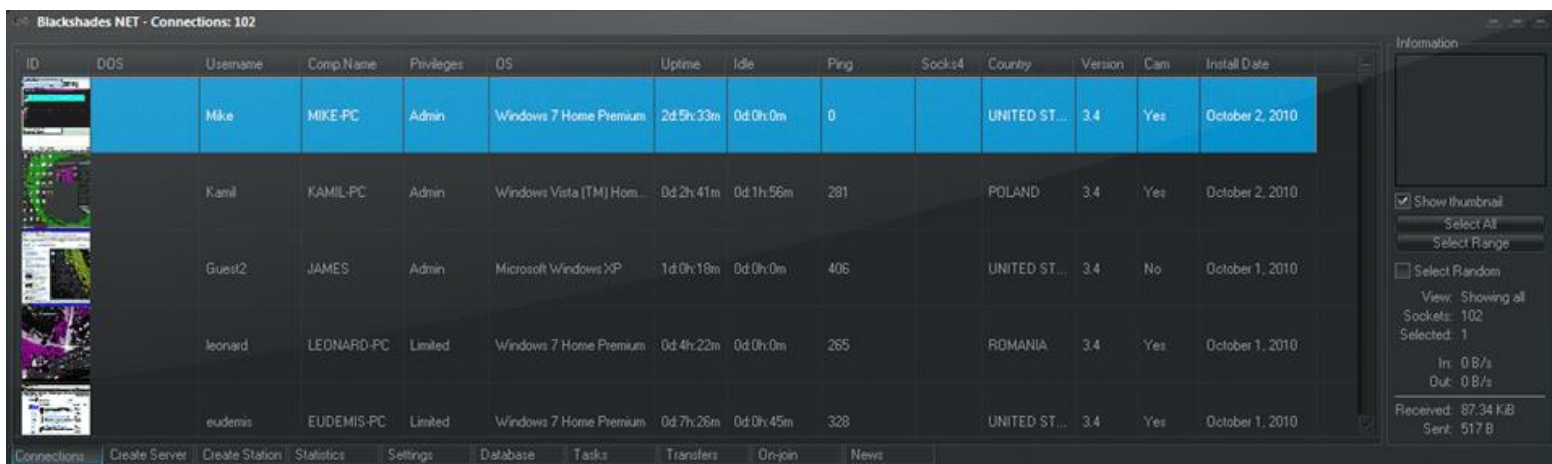
**Get Tons Of
FEMALE SALVES
Now!!**

- ✓ HOT FEMALESLAVES FAST!
- ✓ ALMOST JUST COPY&PASTE
- ✓ TIPS AND TRICKS
- ✓ INSTANT SETUP

CLICK HERE

Some RATs for demonstrations

Blackshades NET

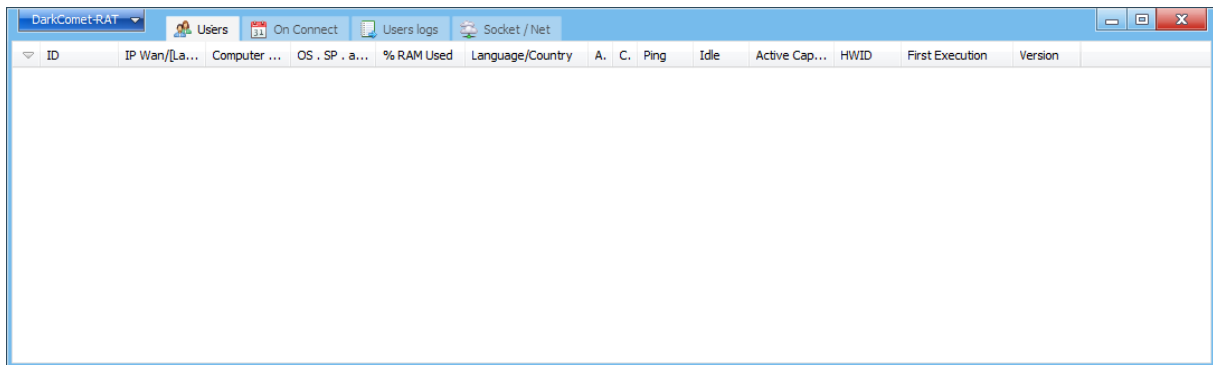


The Blackshades Team are one of the people who dominate the RAT market, they already code for several years and they have many unique features in their programs.

What speaks for Blackshades NET:

- **Thumbnail Viewer – Check the file before you download it!**
- **Torrent Seeder**
- **It's stable**
- **Webserver – You can control your Victim from any kind of device, like an Iphone.**
- **Live Keylogger – It will send the typed keystrokes immediately to you**
- **Multi Transfer – Download more than just one file at once!**

DarkComet

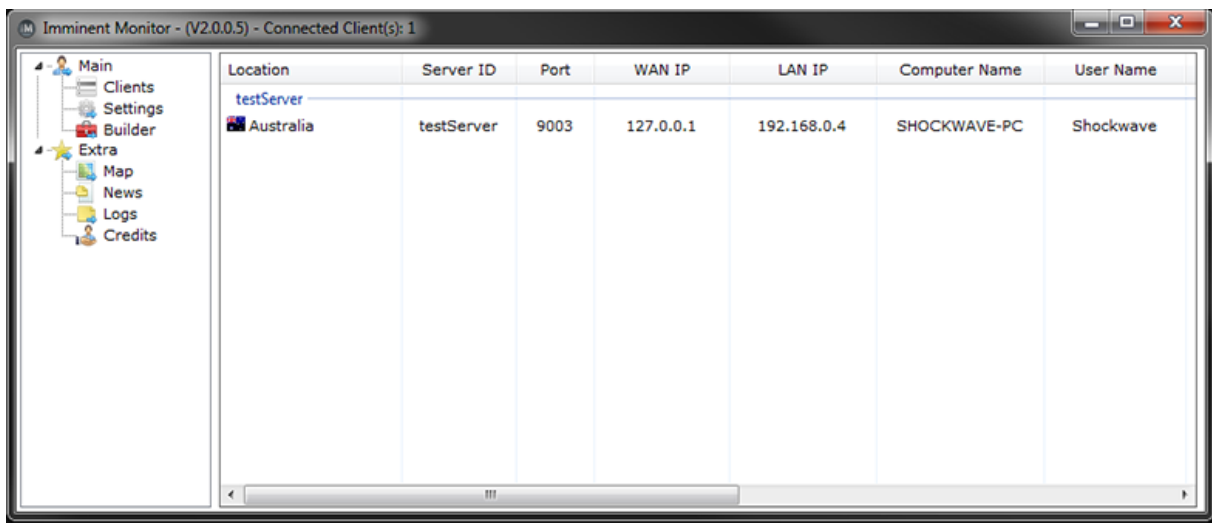


DarkComet is one of the old rabbits. Unfortunately the developer won't update his product anymore. But it's still one of the most effective RATs out there

What speaks for DarkComet 5.3.1:

- **It's free**
- **Still one of the best RATs out there although I hasn't been updated for almost a year.**
- **Stable Webcam, Desktop recorder**
- **Almost every Crypter supports it**

Imminent Monitor



Imminent Monitor is the youngest RAT compared to the others here. It's very fast and effective and I think it will be one of the best RATs after version 3 comes out.

What speaks for Imminent Monitor:

- **It's not that expensive, 20\$**
- **It's fast as fuck, you can view Screens with almost 50 FPS**
- **It's stable**
- **Integrated No-IP Updater**
- **Registry Manager**
- **Thumbnail Viewer**
- **With Version 3 there will be many features which will bring the RAT to one of the best on the market**

How to configure a RAT

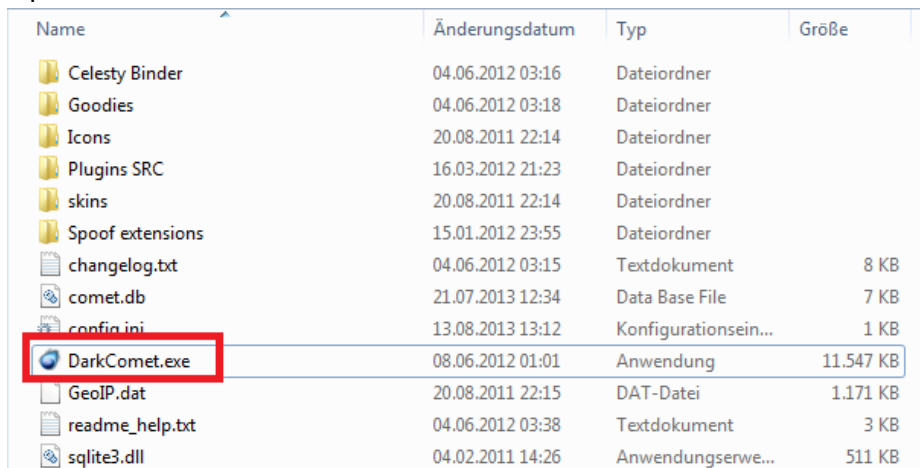
Now we come to the part where it will be exciting. We configure the RAT. Every example I show here is made with DarkComet 5.3.1. Why? Because it's for free, everyone can have it and is newbie friendly!

You can Download DarkComet 5.3.1 here:

You have to deactivate your Anti-Virus otherwise it will be detected as virus and you can't open it! Don't be afraid, it's NOT really a virus, but the antivirus companies detect it as one because of the suspicious function you can do with it.

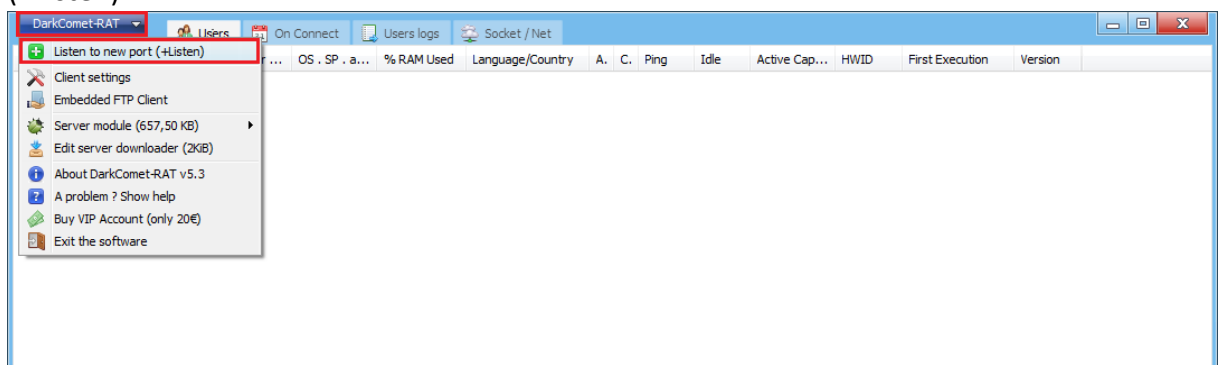
At first you have to choose a port. If you don't know what a port is, it's something like a gate, every connection goes through a port. If the port is not open, then the connection can't come to your PC, it's a security mechanism of your router

1. Extract the Rar files in a folder
2. Open DarkComet.exe

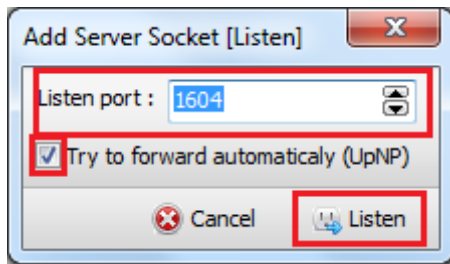


Name	Änderungsdatum	Typ	Größe
Celesty Binder	04.06.2012 03:16	Dateiordner	
Goodies	04.06.2012 03:18	Dateiordner	
Icons	20.08.2011 22:14	Dateiordner	
Plugins SRC	16.03.2012 21:23	Dateiordner	
skins	20.08.2011 22:14	Dateiordner	
Spoof extensions	15.01.2012 23:55	Dateiordner	
changelog.txt	04.06.2012 03:15	Textdokument	8 KB
comet.db	21.07.2013 12:34	Data Base File	7 KB
config.ini	13.08.2013 13:12	Konfigurationsein...	1 KB
DarkComet.exe	08.06.2012 01:01	Anwendung	11.547 KB
GeoIP.dat	20.08.2011 22:15	DAT-Datei	1.171 KB
readme_help.txt	04.06.2012 03:38	Textdokument	3 KB
sqlite3.dll	04.02.2011 14:26	Anwendungserwe...	511 KB

3. Click on the left Corner on "Darkcomet-Rat" and then click on "Listen to new port (+Listen) "

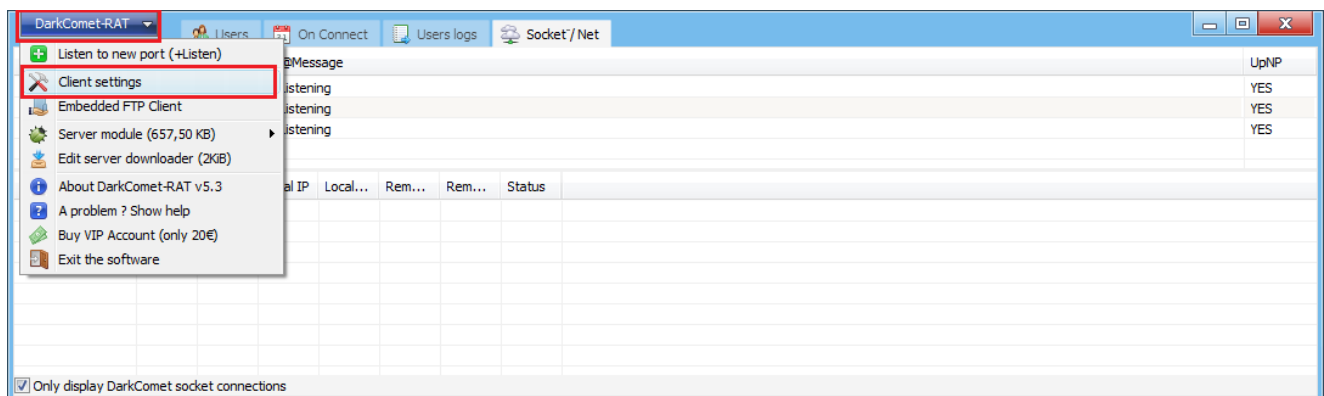


4. After that, a new windows appears, there is already a number in it, which is a standard value, I recommend not to use the standard one, because many newbies use it, you should choose something like 1733, 1943 or 1253, something that isn't common when you open ports, make sure "Try to forward automatically (UpNP)" is marked, after you choosed one, click on "Listen".

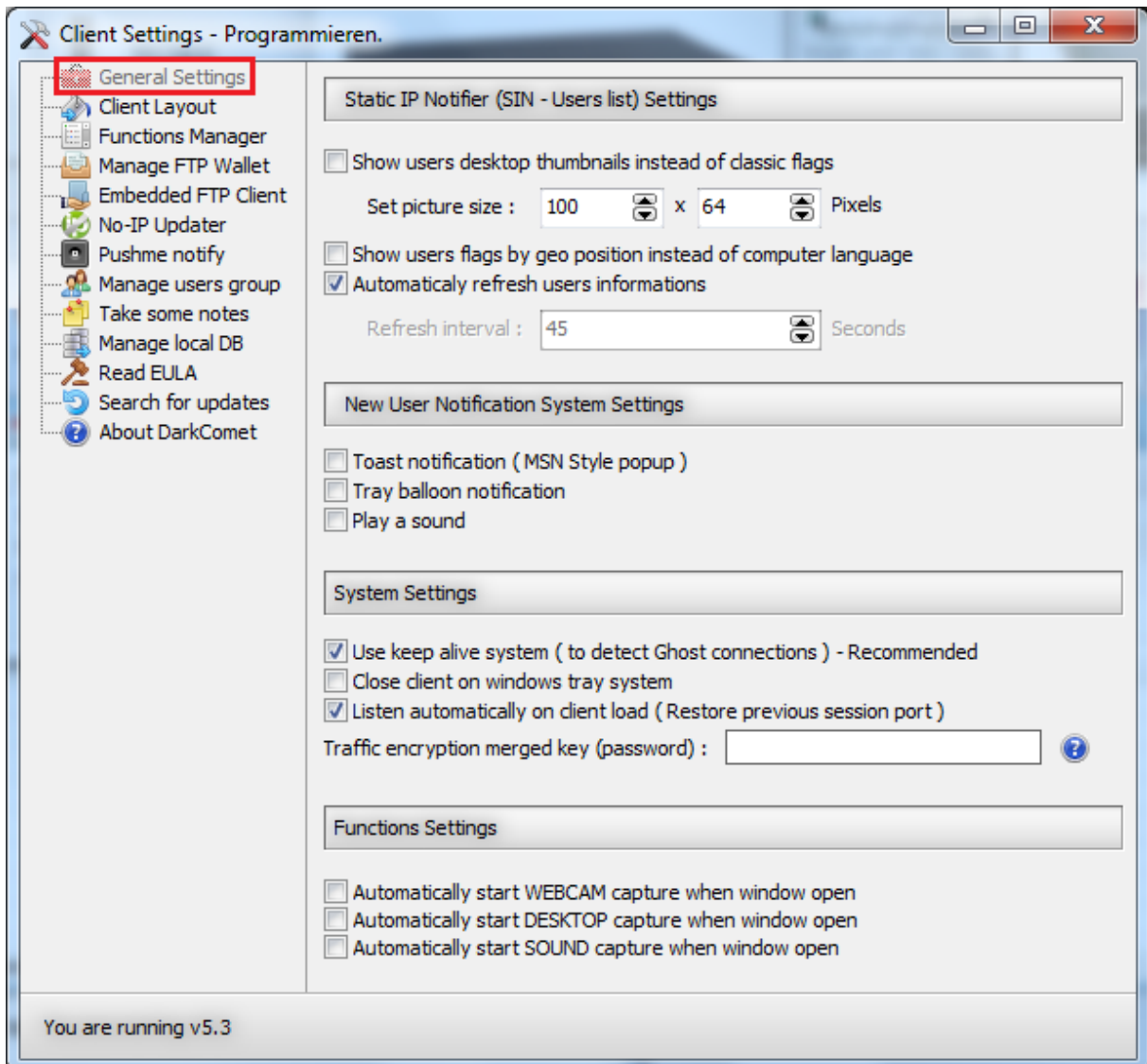


But why you can't use the standard port? As I already said, many other users use this port, so they opened this port. If your last connection with a VPN is saved in a DNS and you log off, someone else can use the VPN IP Address, if he now uses DarkComet and has opened the standard port too, he can see your slaves and also he can steal them! That's something we don't want, right?

5. Now Click again on the left Corner on "Darkcomet-Rat" and then click on "Client Settings"



6. Now click on "General Settings" and do the settings like me.

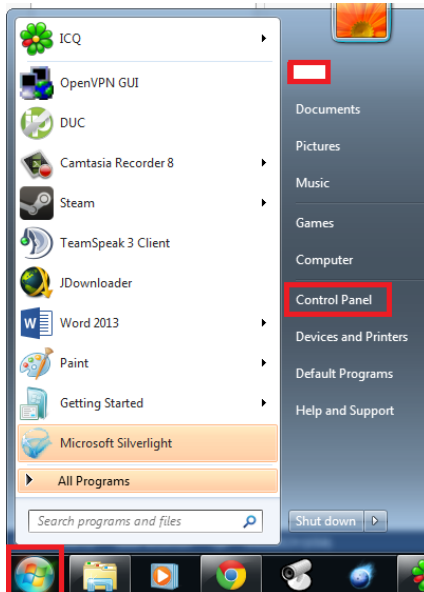


Now you finished the settings for DarkComet, now we come to the next part, the Port Forwarding.

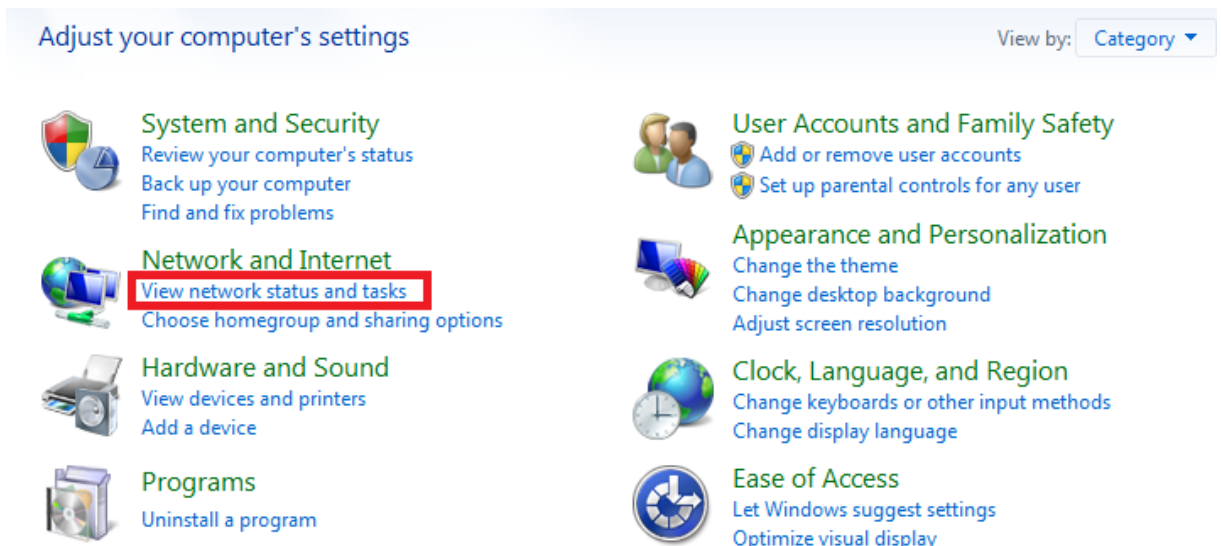
How-To configure your Computer

So, now we need a static IP in your Computer, we need it for the case if you want to rat with your own IP, without a VPN. I also do this often, I have an extra DNS where I put slaves which I want to research particularly. The connection is faster, you can transfer files faster and you can have a better Webcam quality.

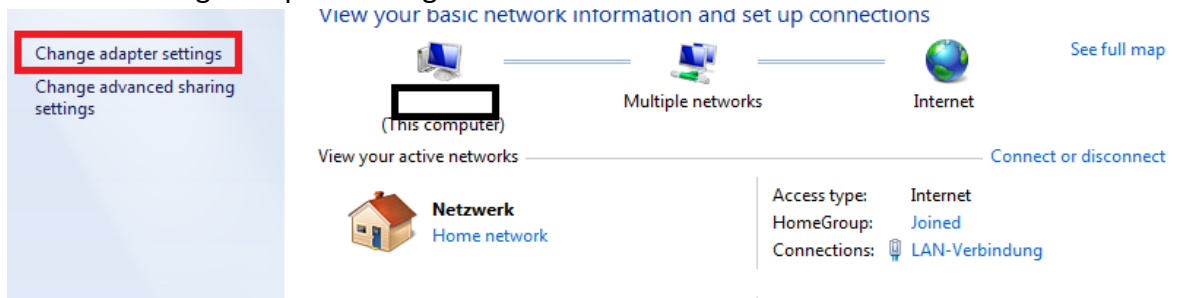
1. Click on "Start" and "Control Panel"



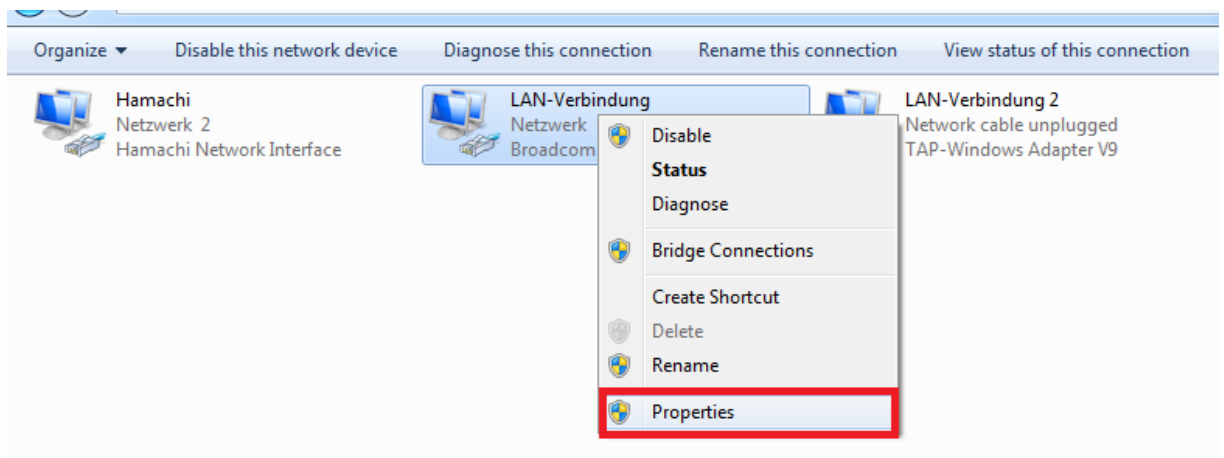
2. Click on "View network status and tasks"



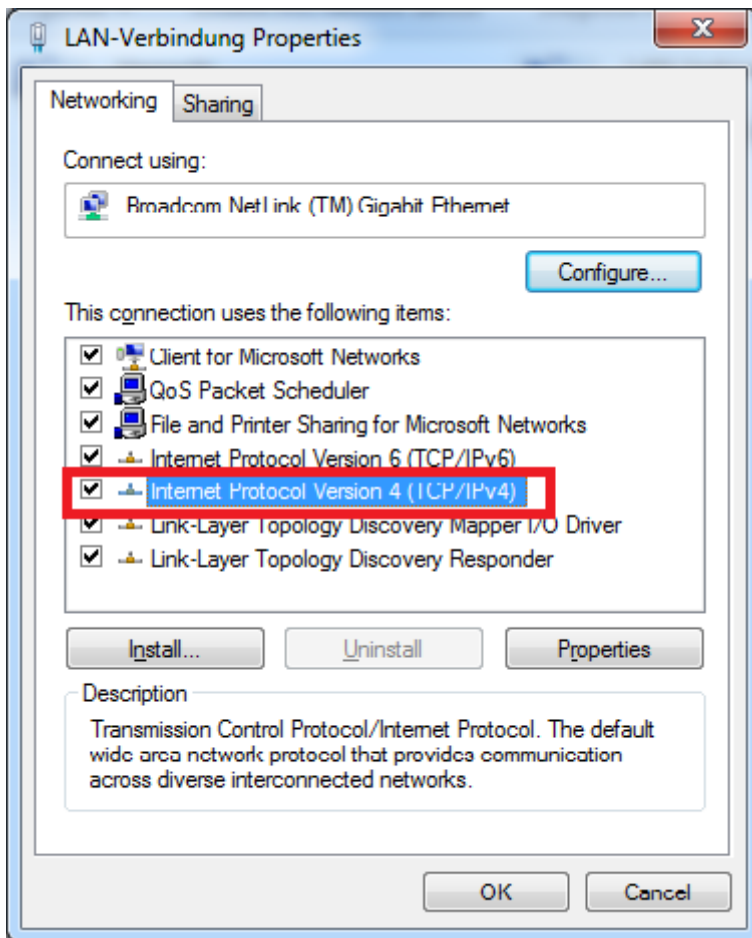
3. Click on "Change Adapter Settings".



4. Right click on your LAN-Connection and click "Properties"



5. Double left click on “Internet Protocol Version 4 (TCP/IPv4)”



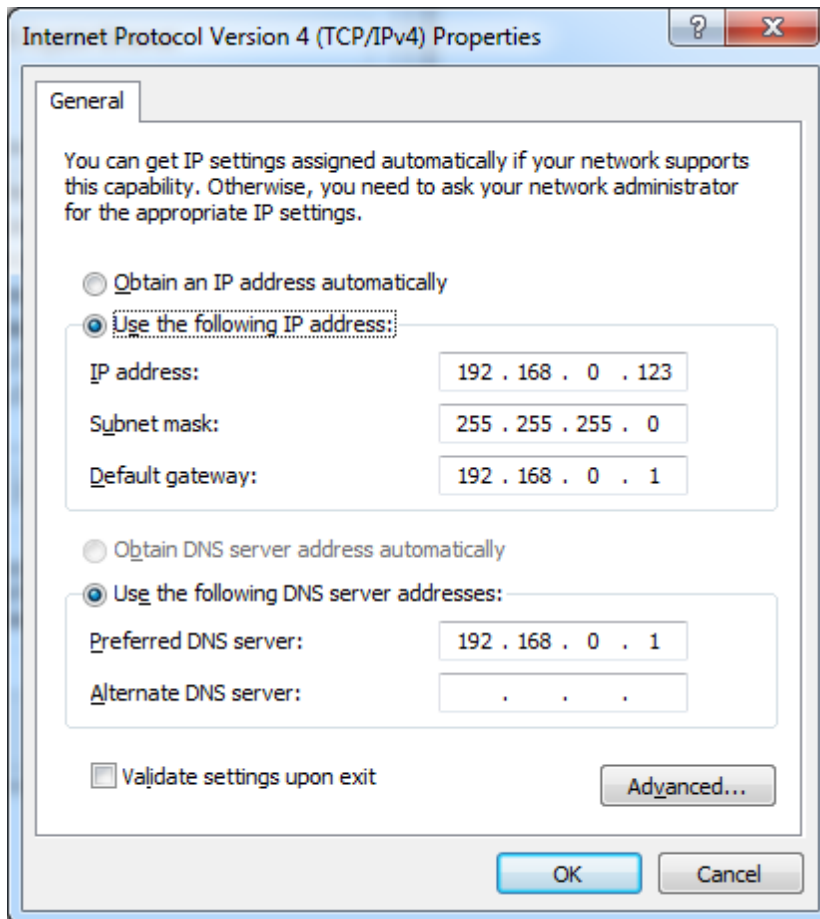
6. Now you see some fields, mark the box “Use the following IP Address:” and fill it like this:

IP Address: 192.168.0.123 (This will be your static IP, we need it later to Port Forward)

Subnet mask: 255.255.255.0

Default Gateway: The IP which you can connect to your router (if you don't know it, open your cmd under Start -> “CMD” in the search field and type ipconfig /all and search for “Default Gateway” in “Lan-Connection”)

Preferred DNS-Server: Same as Gateway



Your PC now should be configured for the case you want to RAT with your Real IP!

Port Forwarding

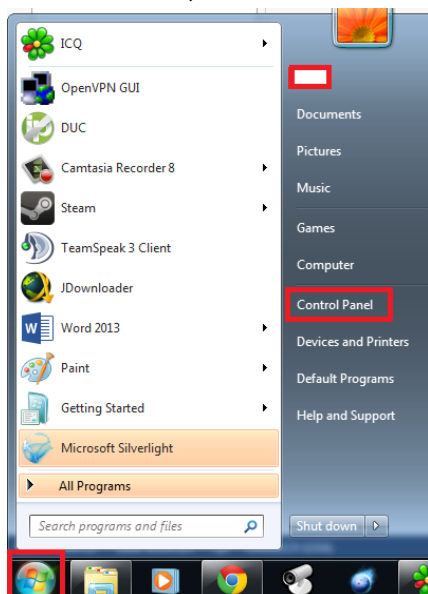
Now we come to the funny part, Port Forwarding is one of those things where every newbie has problems with it. Why do we need this? We now have already configured a port in Darkcomet, imagine a guy who stands at the end of a tunnel, he watches if someone comes through the tunnel, but at the other side, the tunnel is closed and no one can come through the tunnel. So we have to open that tunnel, that is what Port Forwarding is. You open the Port, so a connection can go through this tunnel.

Useful links: <http://www.canyouseeme.org/> - Here you can check if the port is open.

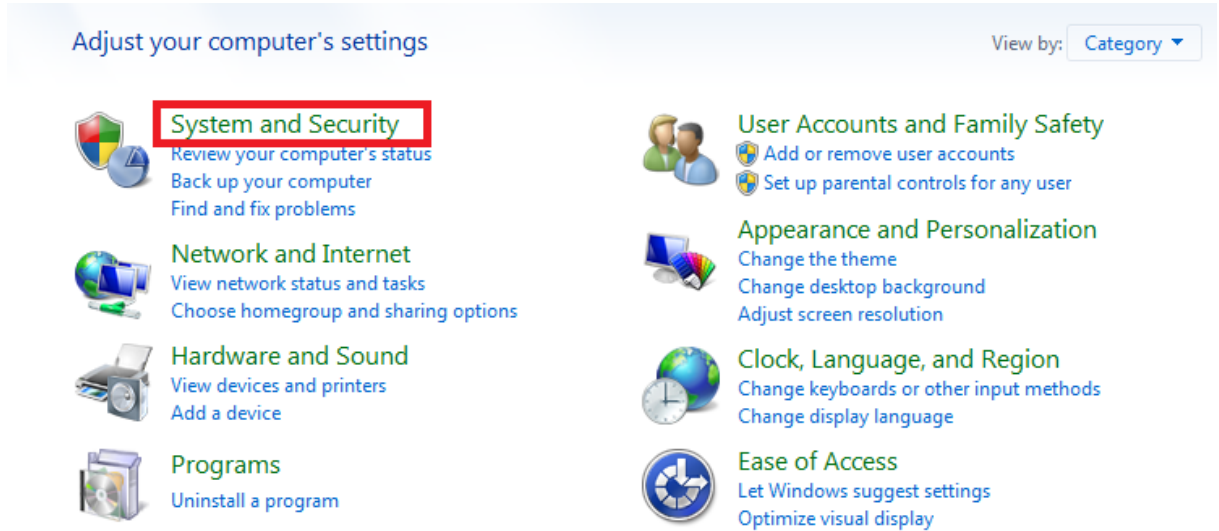
Deactivating Windows Firewall

At first you have to deactivate your Windows Firewall, so there will be no problem with the connections

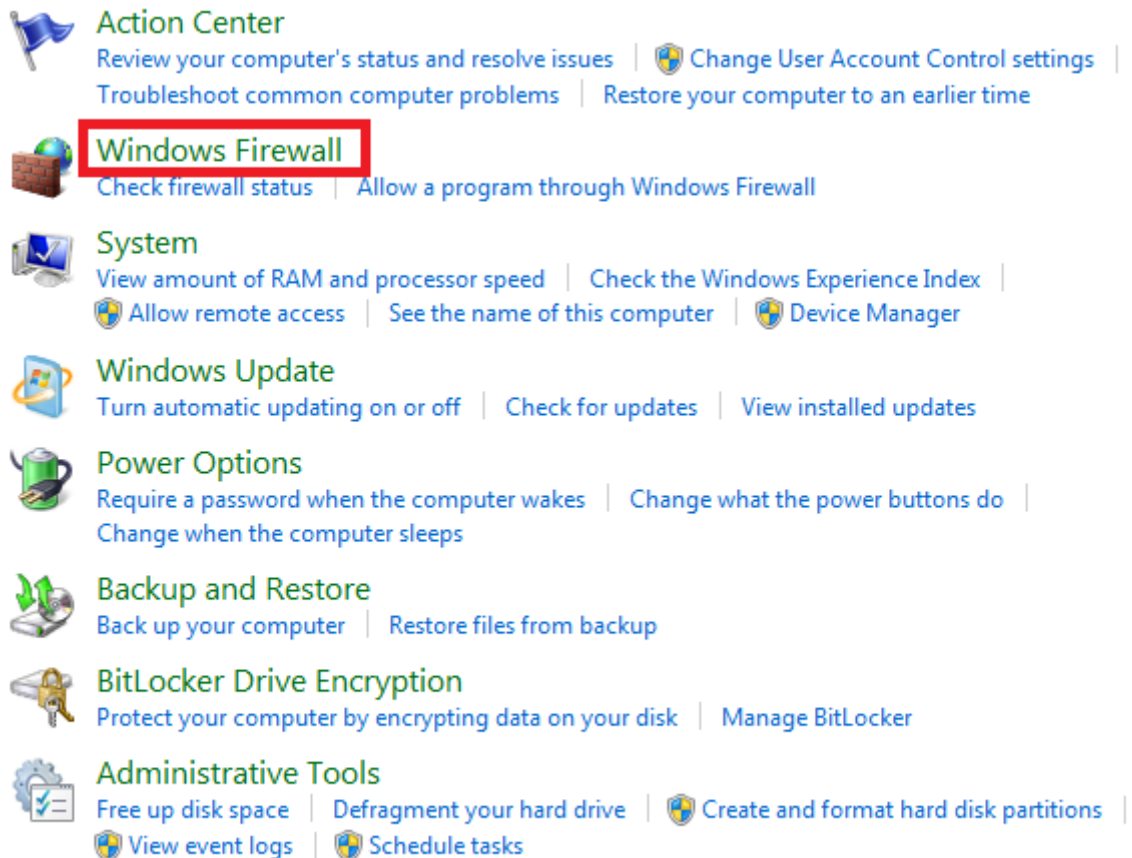
1. Click on "Start", then on "Control Panel"



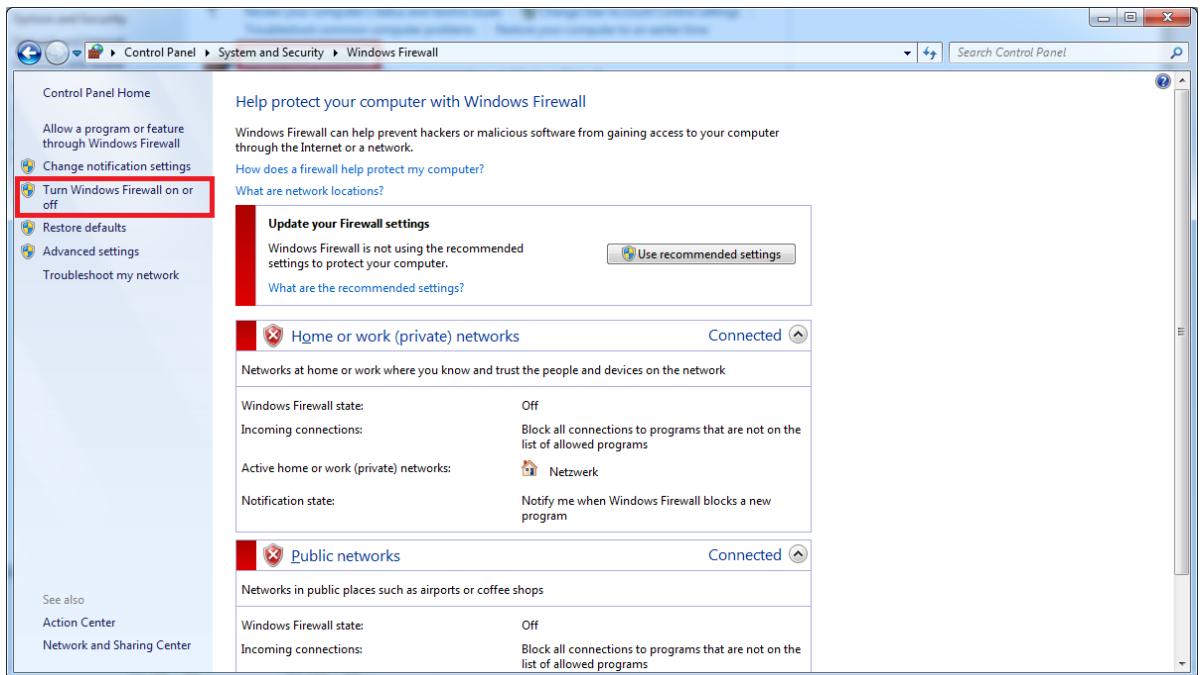
2. Click on "System and Security"



3. Click on "Windows Firewall"



4. Now Click on “Turn Windows Firewall on or off”



5. Now mark both points at “Turn off Windows Firewall”

Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

- Turn on Windows Firewall
 - Block all incoming connections, including those in the list of allowed programs
 - Notify me when Windows Firewall blocks a new program
- Turn off Windows Firewall (not recommended)

Public network location settings

- Turn on Windows Firewall
 - Block all incoming connections, including those in the list of allowed programs
 - Notify me when Windows Firewall blocks a new program
- Turn off Windows Firewall (not recommended)

The Windows Firewall shouldn't make problems anymore. We have a free way for our connections!

Port Forwarding with your router

No it will be a little bit tricky because not every router is like the other. I can only do it with my router, I will show you for what you have to look!

If you have a different router or maybe don't understand my tutorial then you should look here:

http://portforward.com/english/routers/port_forwarding/

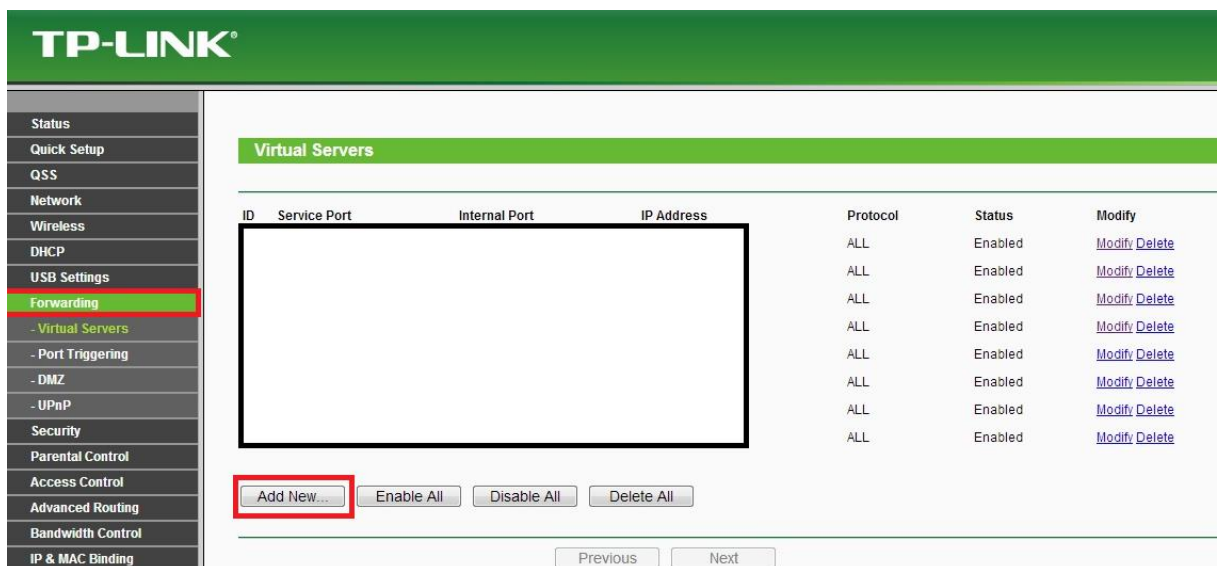
Here are Port Forwarding tutorials for nearly every router on the market.

I will show you the tutorial with a TP-Link router.

At first search for your router IP address, you can find it with the cmd

Click on the Windows Start button and search for "cmd" and open it. After that you type "ipconfig /all". Now search the Gateway Address in "LAN-Connection"

1. Connect to your router with the IP Address you found.
2. Search for something like Forwarding or Port Forwarding. After that, click on "Add New..."



TP-LINK

Virtual Servers

ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
				ALL	Enabled	Modify Delete
				ALL	Enabled	Modify Delete
				ALL	Enabled	Modify Delete
				ALL	Enabled	Modify Delete
				ALL	Enabled	Modify Delete
				ALL	Enabled	Modify Delete
				ALL	Enabled	Modify Delete

3. Fill it with the informations.

The screenshot shows the TP-LINK web interface. On the left is a sidebar menu with the following items: Status, Quick Setup, QSS, Network, Wireless, DHCP, USB Settings, Forwarding (highlighted in green), - Virtual Servers, - Port Triggering, - DMZ, - UPnP, Security, and Parental Control. The main content area is titled 'Add or Modify a Virtual Server Entry'. It contains the following fields and controls:

- Service Port: (XX-XX or XX)
- Internal Port: (XX, Only valid for single Service Port or leave it blank)
- IP Address:
- Protocol:
- Status:
- Common Service Port:
- Buttons: and

Service Port: Write the Port in this box with your DarkComet is listening to (See.: How to configure your RAT)

Internal Port: Same as Service Port

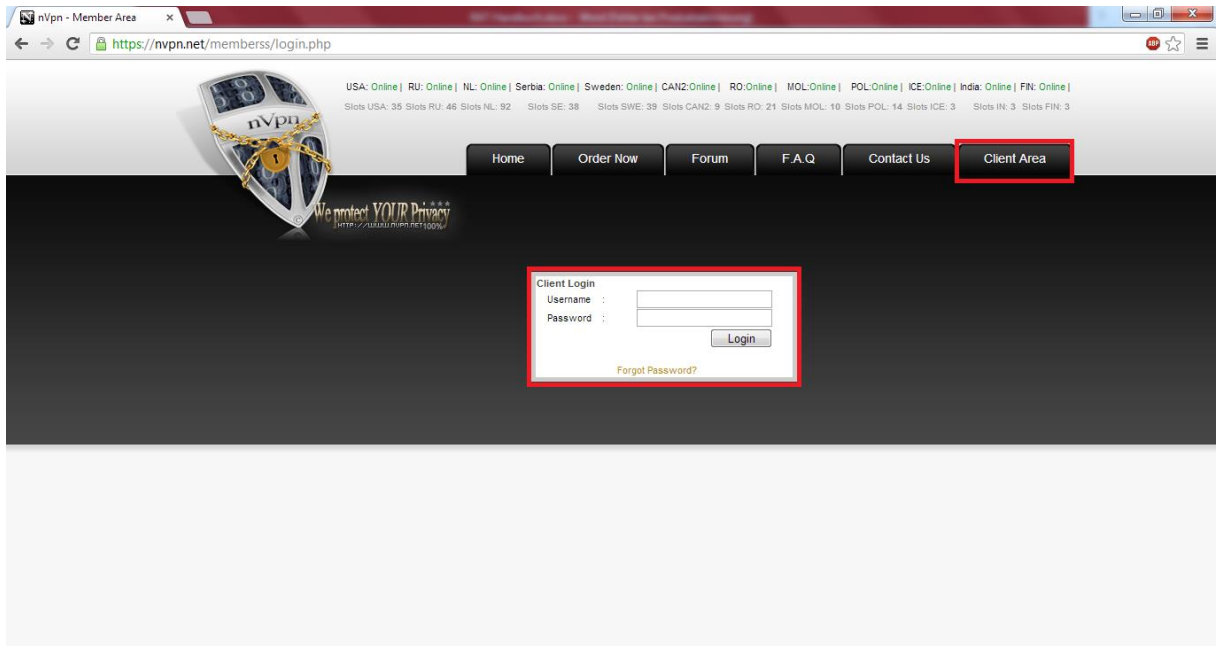
IP Address: The static IP Address of your Computer (See.: How to configure your Computer)

Then you just have to click on "Save". Now your port should be open, test it on canyouseeme.org

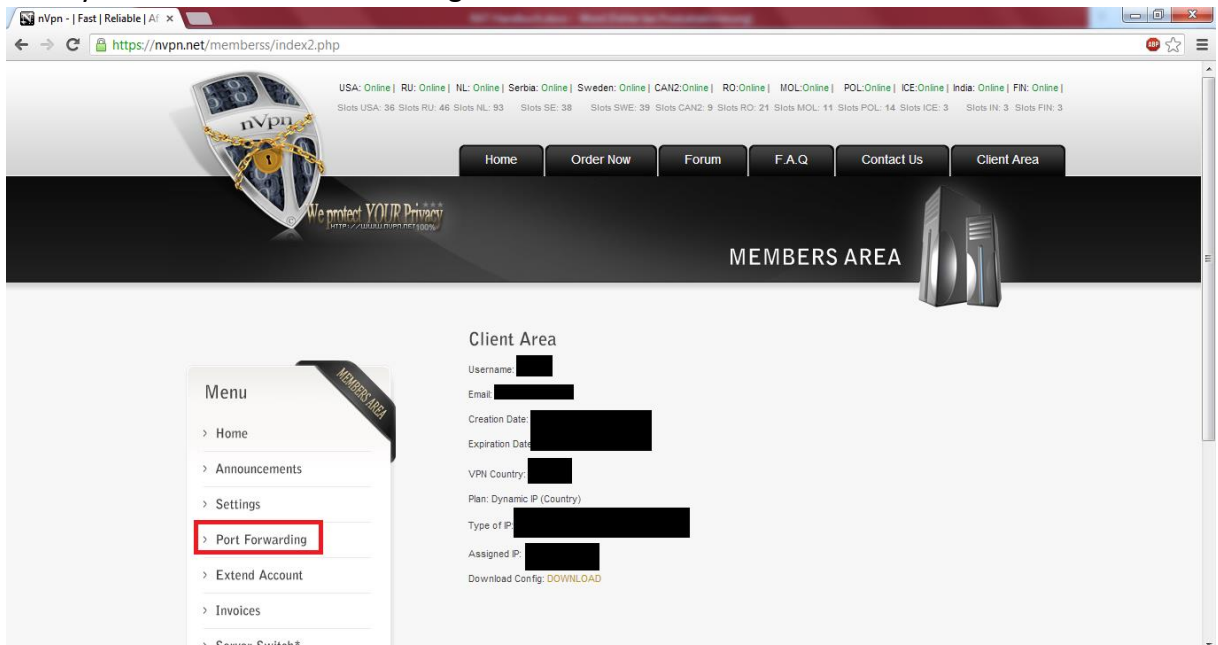
Port Forwarding with your VPN (NVPN)

So, as I recommend, you should be always online with a VPN when you do anything what is related to raiting. If you use your VPN for raiting, then we have to Port Forward in VPN Provider, I will show you it with the VPN Provider <http://NVPN.Net>.

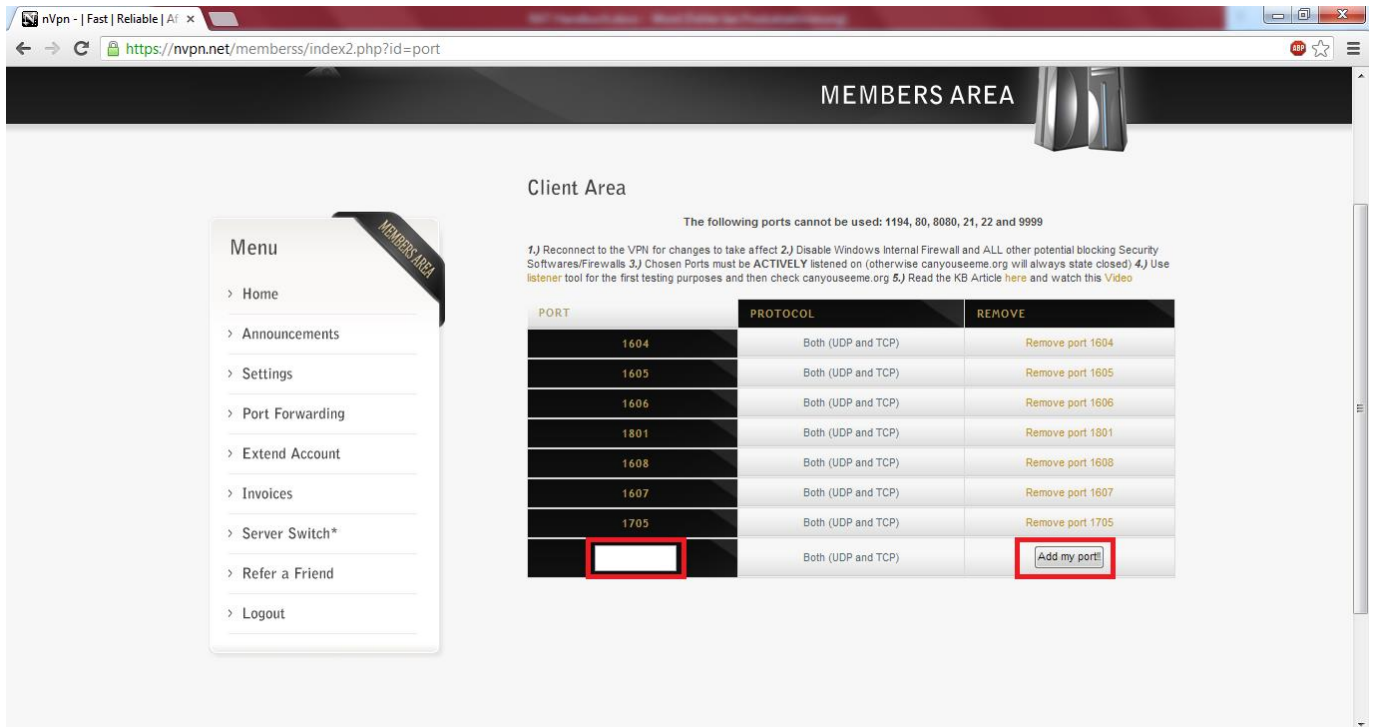
1. Go to the website NVPN.net
2. Log into your account



3. Then you click on "Port Forwarding"



4. Here you can see the overview of ports that are already forwarded. Now you can write your Port, which you choosed in DarkComet earlier, in the first column, after that click on "Add my port!!".



The screenshot shows the 'MEMBERS AREA' of nVpn.net. On the left is a 'Menu' with options: Home, Announcements, Settings, Port Forwarding, Extend Account, Invoices, Server Switch*, Refer a Friend, and Logout. The main content is the 'Client Area', which includes a warning: 'The following ports cannot be used: 1194, 80, 8080, 21, 22 and 9999'. Below this is a table of forwarded ports:

PORT	PROTOCOL	REMOVE
1604	Both (UDP and TCP)	Remove port 1604
1605	Both (UDP and TCP)	Remove port 1605
1606	Both (UDP and TCP)	Remove port 1606
1801	Both (UDP and TCP)	Remove port 1801
1608	Both (UDP and TCP)	Remove port 1608
1607	Both (UDP and TCP)	Remove port 1607
1705	Both (UDP and TCP)	Remove port 1705
<input type="text"/>	Both (UDP and TCP)	<input type="button" value="Add my port!!"/>

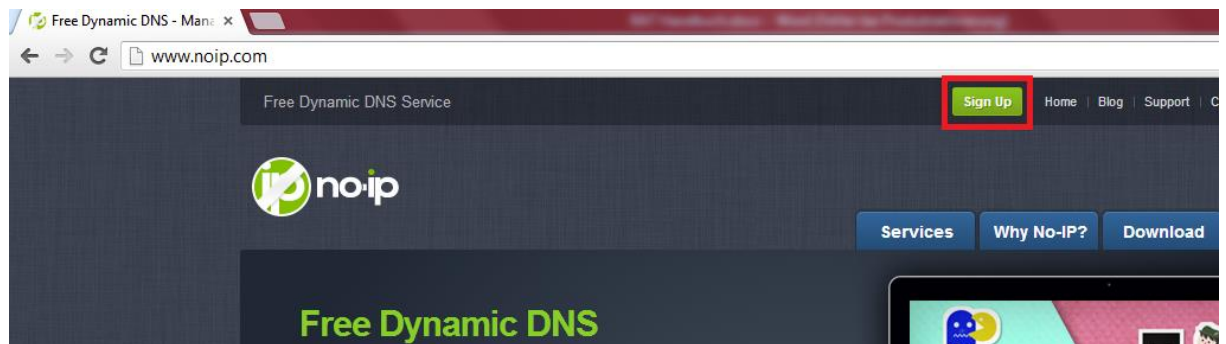
You now should have successfully opened the port for your VPN! Start your VPN and test it on canyouseeme.org

NO-IP & DUC (Dynamic Update Client)

What is No-IP? No-IP is a website where you can generate a dynamic DNS (**D**omain **N**ame **S**ystem), you can surely remember that we choosed a dynamic IP when we ordered a VPN, now you should think about the connection. We can't use only one IP when we build a RAT file, instead of a pure IP, we want to use a DNS, you can upgrade a DNS with every IP you want. It's like an empty value, which you can fill with an IP Address, another benefit is, we don't have to use a real IP on your RAT, so it's not so easy to read your IP out of the program.

We have to register on <http://www.noip.com/>, if it's already possible for you, you should use your VPN, just for your safety!

1. Go on the website noip.com
2. Click on "Sign up"



3. Now you should go on this site <http://10minutemail.net> . There you can make a 10 minute Email. **ATTENTION:** It could be possible that you need this E-Mail Address later again, so save the Address in a text editor file.

4. Now fill the empty fields. You have to use a Username, a password, the 10 Minute E-mail Address and a Hostname. In the Hostname field, you have to type a random name, like "Mouse2" or "House1", anything you want, I recommend that you don't use a long word. The Hostname is the DNS Address.

Create Your No-IP Account

Username: Usernames must be 6-15 characters long and only contain a-z,0-9, -, and _

Password:
Confirm Password: Minimum of 6 characters.
Password Strength

Email: We will be sending an account activation link, so please be sure your email is correct.

Hostname: .no-ip.biz Choose a hostname for your account. You can change your hostname or add more later.
 Create my hostname later

5. Now you have to activate your Account in your 10 Minute Email Address, don't worry, it should come fast. If not, wait a bit.

6. Now you can log into your Account. You should now have an overview like this:

Your No-IP Account Support Sign Out

Hosts/Redirects DNS Hosting Domain Registration Mail SSL Certificates Monitoring Backup DNS Renew/Activate

Need Help?
Support Center
Troubleshooting Guide
Dynamic Update Client
Support Ticket
Contact Us

Your No-IP
Welcome to your No-IP!

You have successfully logged into No-IP's member section. To start using No-IP's services select an icon below or choose an item from the navigation above.

Manage Domains Add Domain Refer Friend Add a Host Manage Hosts

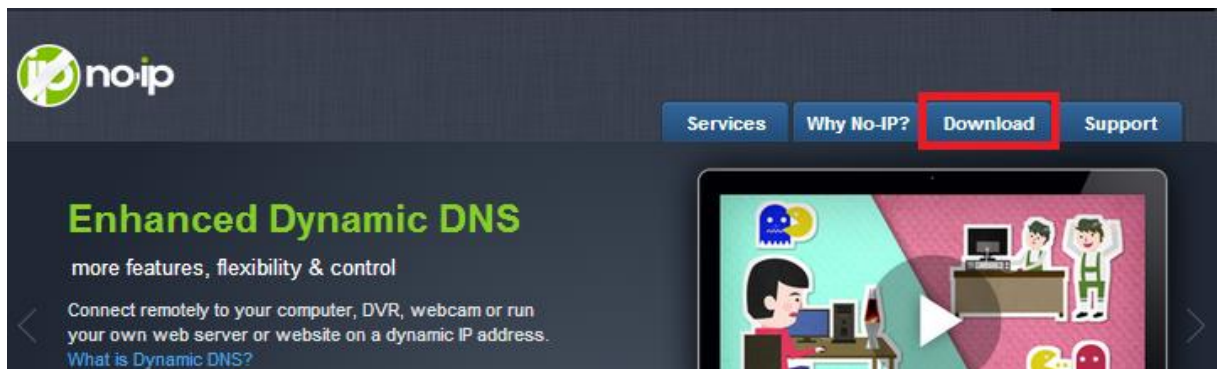
Find a Domain Name com

You can use up to 3 DNS Addresses as a free user, I would recommend you to use all of them, just to be safe that you have a stabile connection. Also, you need one DNS with that you can use your real IP, as I said it above.

If you want to add new DNS Addresses, just click “Add a Host”, if you want to manage them click “Manage Hosts”, the other links should be not of interest for you.

Now we have to download a DUC (Dynmaic Update Client), for our luck, noip offers that program for free.

1. Got to <https://www.noip.com>
2. Click on “Download”

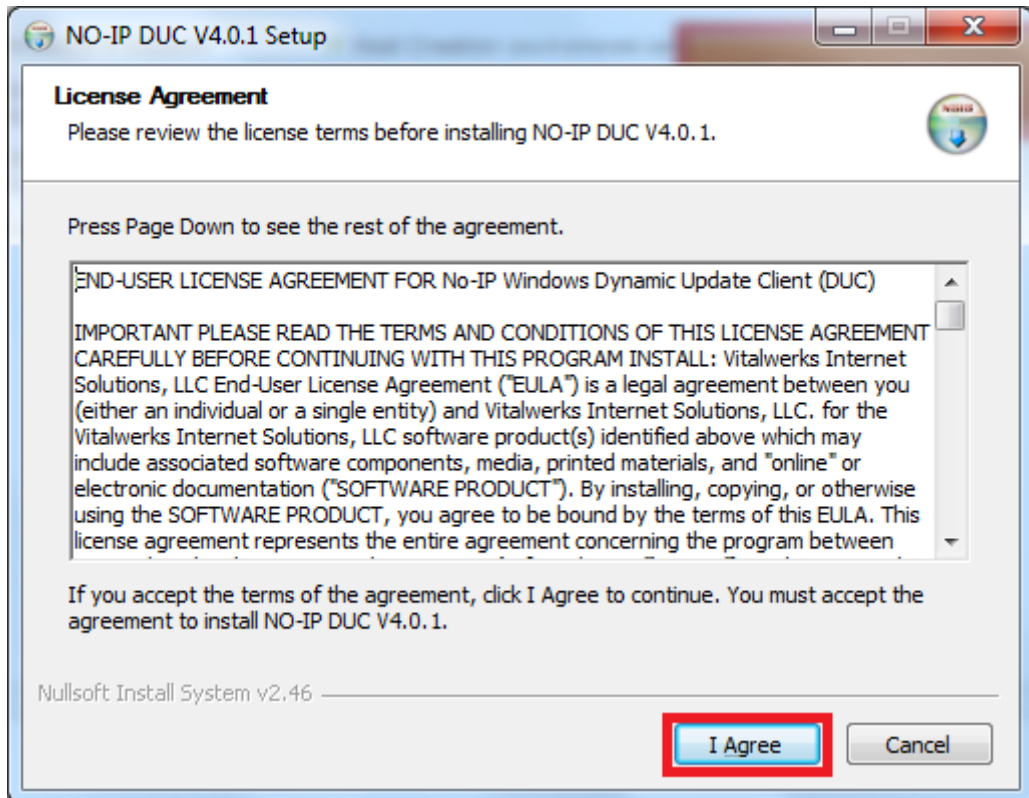


3. Click on “Download now”

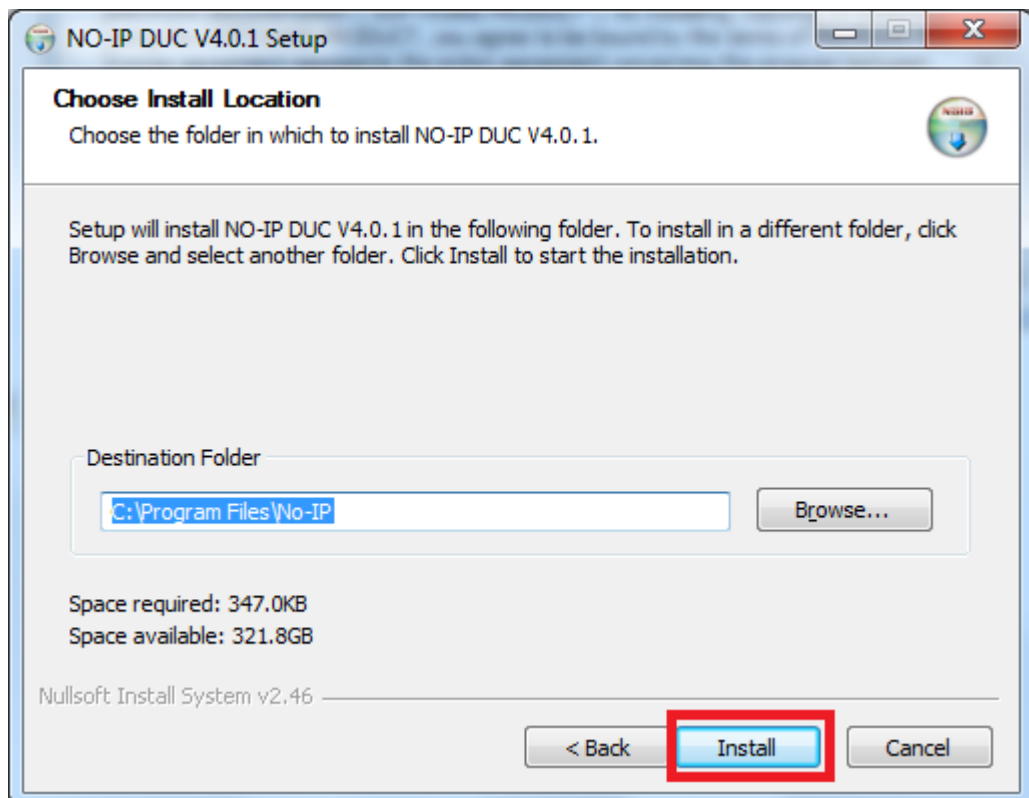
A screenshot of the 'Dynamic Update Client for Windows' download page. The main heading is 'Dynamic Update Client for Windows'. Below it, the section is titled 'Version 4.0.1 Features'. The text describes the client's function: 'Keep your current IP address in sync with your No-IP host or domain with our Dynamic Update Client (DUC). Our dynamic DNS update client continually checks for IP address changes in the background and automatically updates the DNS at No-IP whenever it changes.' A list of features is provided in two columns, each with a green checkmark icon: Windows 8 Support, Secure Key Based Updates, Windows 7 Native Support, Notifications, Host Creation (plus & enhanced user), Light Remote IP Detection, Modern Interface, and Client Tracking. A large orange 'Download Now' button is prominently displayed on the right, with 'version 4.0.1' written below it.

4. Wait until the download finished, then start it.

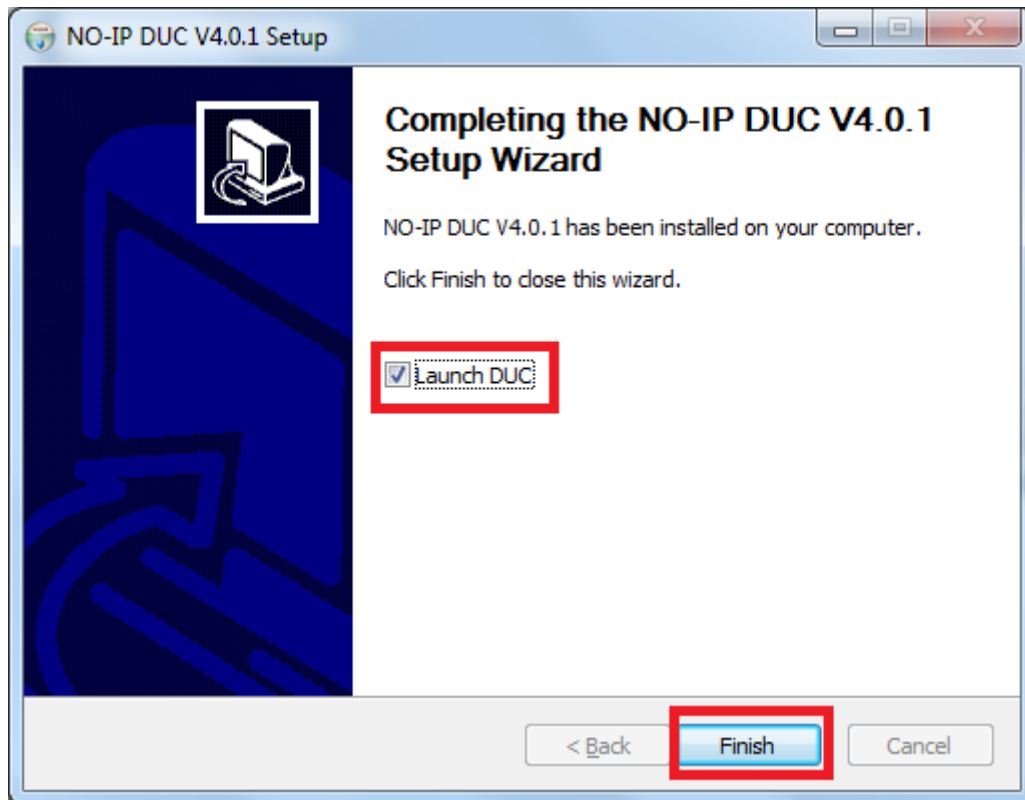
5. Click on "I Agree"



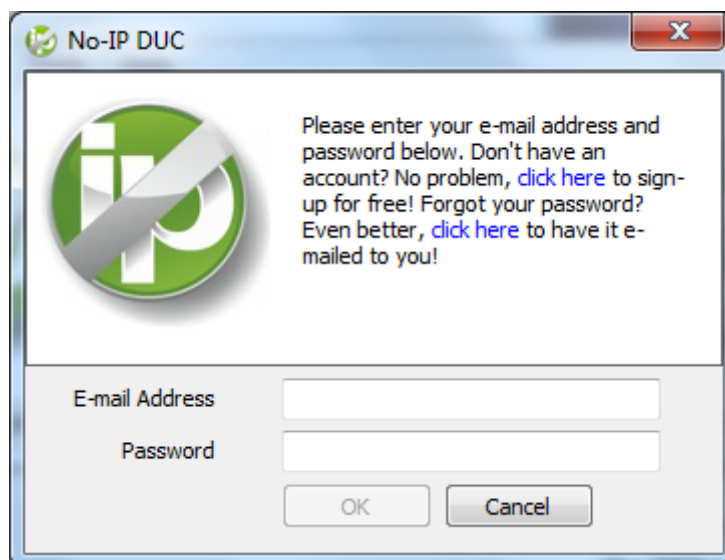
6. Click on "Install"



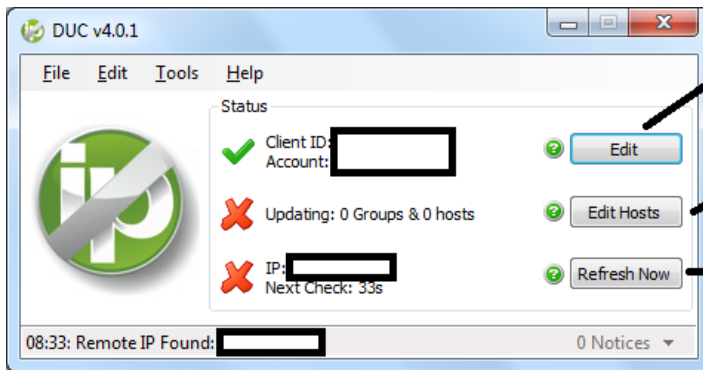
7. Be sure there is mark at "Launch DUC" and click on "Finish".



8. Now you will have the login window below. You can login now, use your Username or the 10 Minute mail as a login name, don't worry, the DNS is not chosen at this time so it will not actualize the DNS with your IP Address. **ATTENTION:** Just chose the DNS when you are already logged into your VPN.



9. You now have Overview like this:

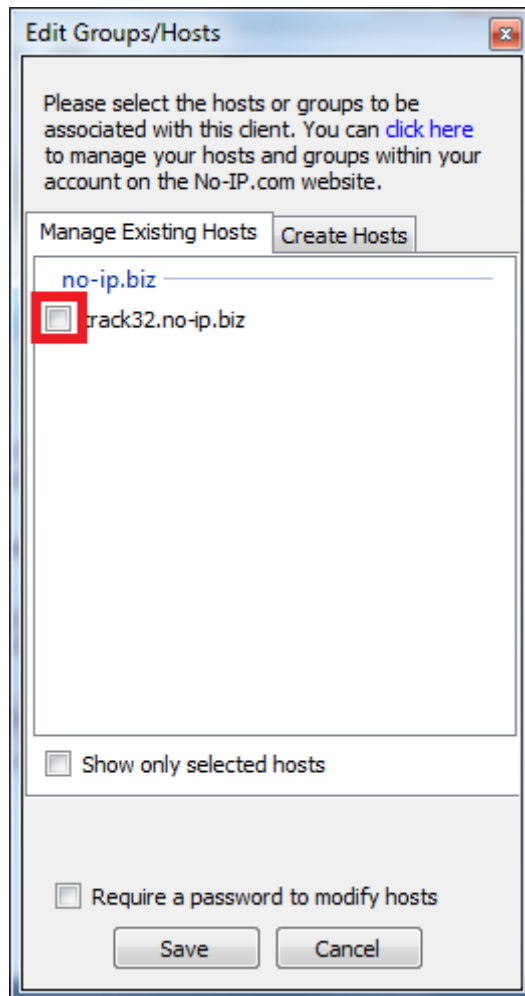


Here you can log into an another account

Here you can chose a DNS which should be upgraded

Here you can refresh your DNS

10. JUST DO THIS STEP WHEN YOU ARE LOGGED INTO YOUR VPN! Click on "Edit Hosts" in your DUC Overview, you should now have window like this:



Here you have an overview of your DNS that you created. If you want to actualize a DNS just be sure that the box behind the DNS is marked. Then click "Save". Congratulations, your DNS is now upgraded with an IP. The DNS will be upgraded all 5 minutes automatically, **so be sure to close your DUC first before you close your VPN.**

How to create a FUD RAT File

Now we should have followed things, be sure, you made everything before you go further:

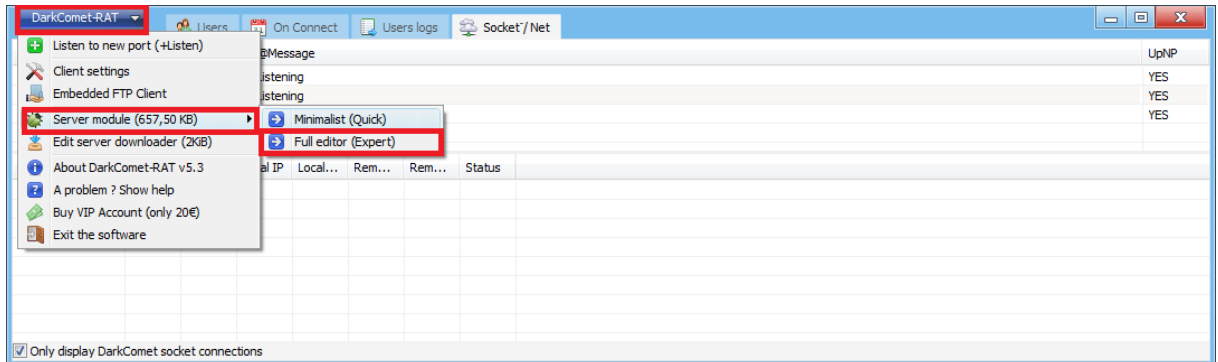
- You have a RAT (DarkComet) and configured the RAT settings.
- You bought a Crypter
- You bought a VPN
- You configured your PC with a static IP
- You Port Forwarded your Ports on your router and VPN
- You registered on Noip.com and created a DNS
- You installed DUC

If you can say to every point a “yes”, then we can go to the next point. Creating a RAT file. I will explain to you how you create a naked RAT file and how you combine it with a Crypter to make it Fully Undetectable (FUD) and how you can't lose a slave.

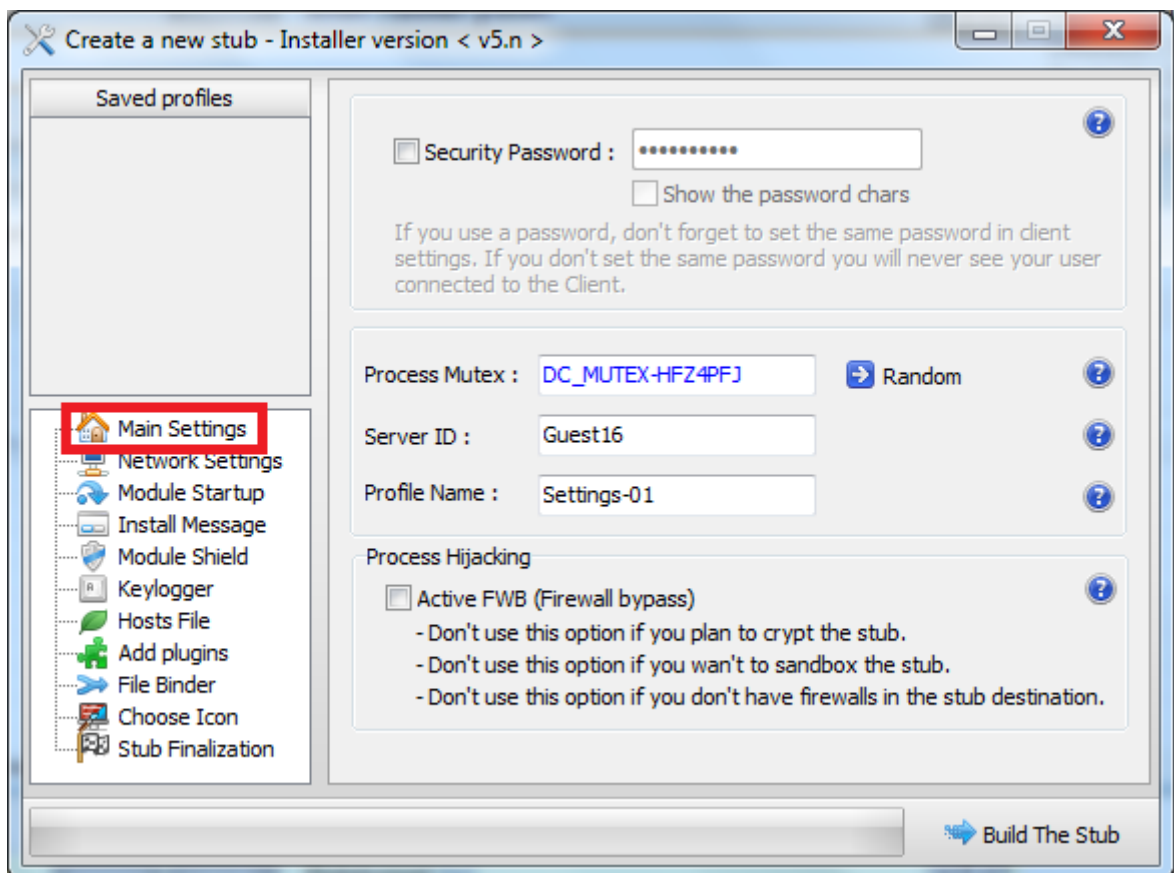
Make a naked RAT file

Why do I call it naked RAT file? Because it's the RAT without any encryption, its naked, it can easily detect by any kind of antivirus.

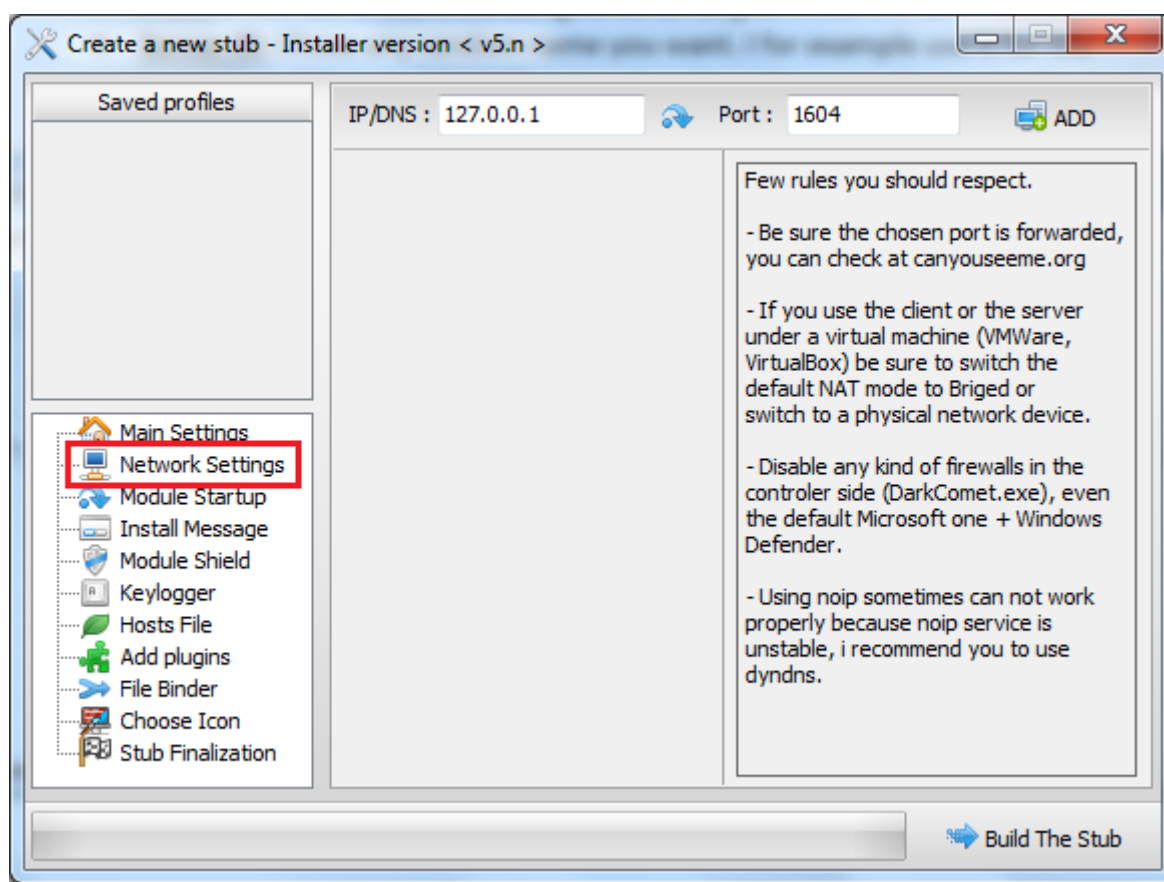
1. Open your DarkComet.exe
2. Now click on "Darkcomet-RAT" in the top corner, after that click on "Server module" - > "Full Editor(Expert)"



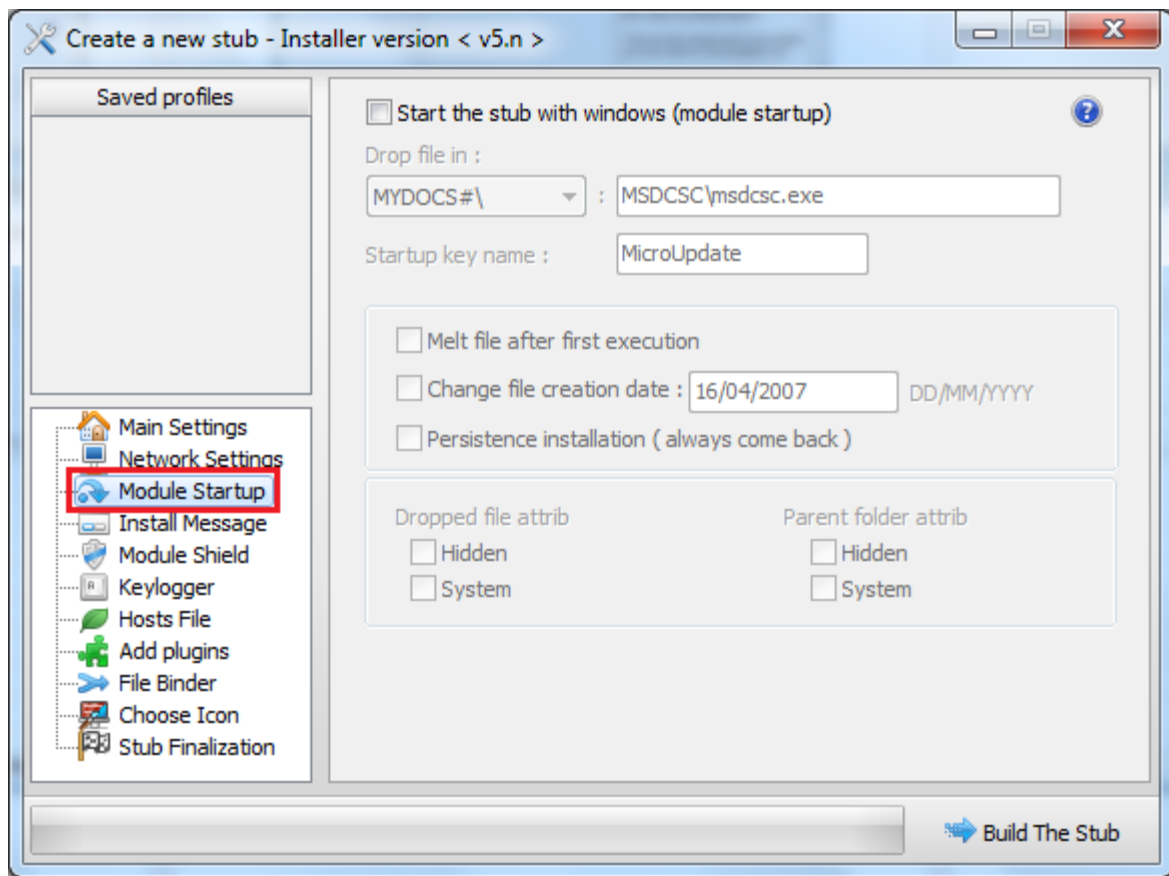
3. A new window should now have opened, configure exact like I say:



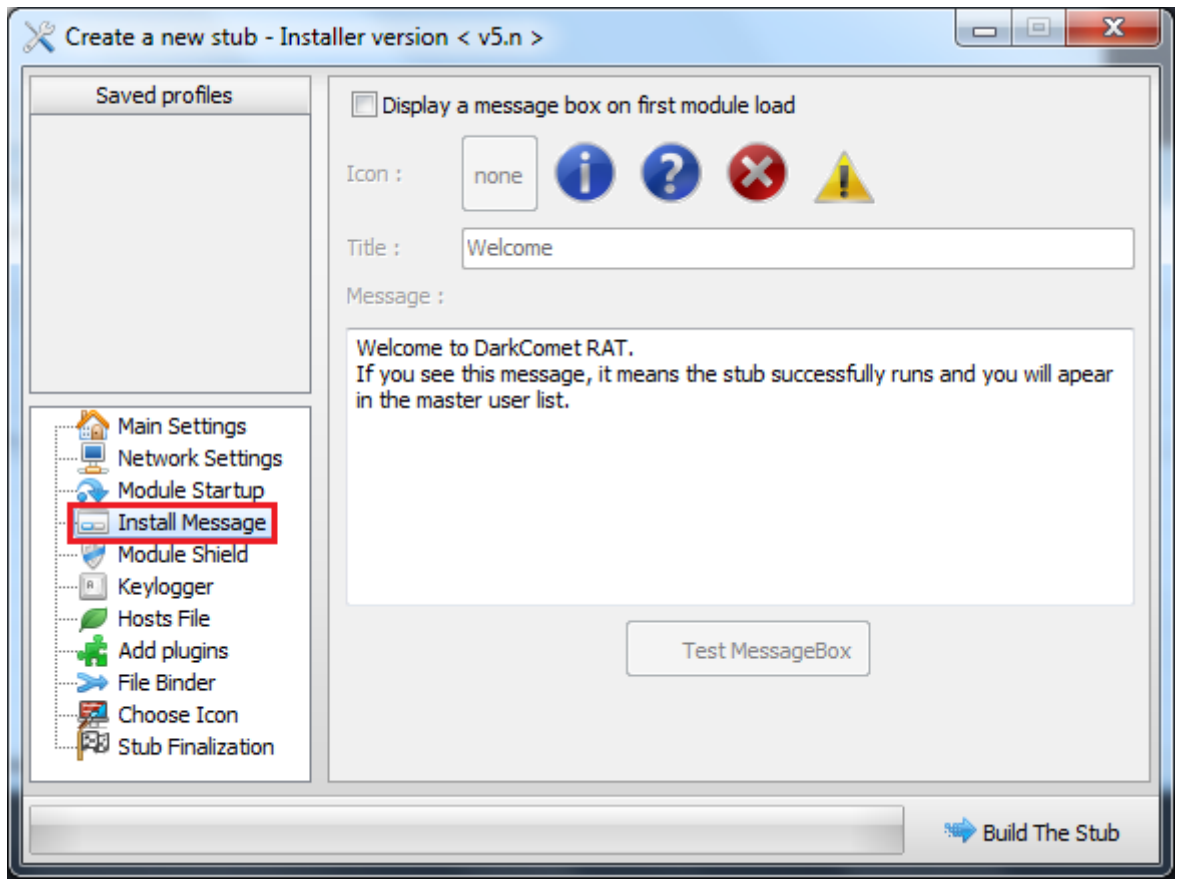
- **Security Password:** Make sure there is no mark in the box.
- **Process Mutex:** Click several times on Random, a Mutex is something like an unique code. It helps you not to install the same rat twice, so if you upload & execute the same rat, it will be ignored as long as it has the same Mutex ID.
- **Server ID:** Chose any random name you want. I for example use it for the logistic, I build a naked RAT file everyday where I'm spreading, so I call it 14.8 or 15.8, it depends which date it is where I'm spreading.
- **Profile Name:** You can save your setting, there you can chose your profile name
- **Process Hijacking:** Make sure there is no mark in the box.



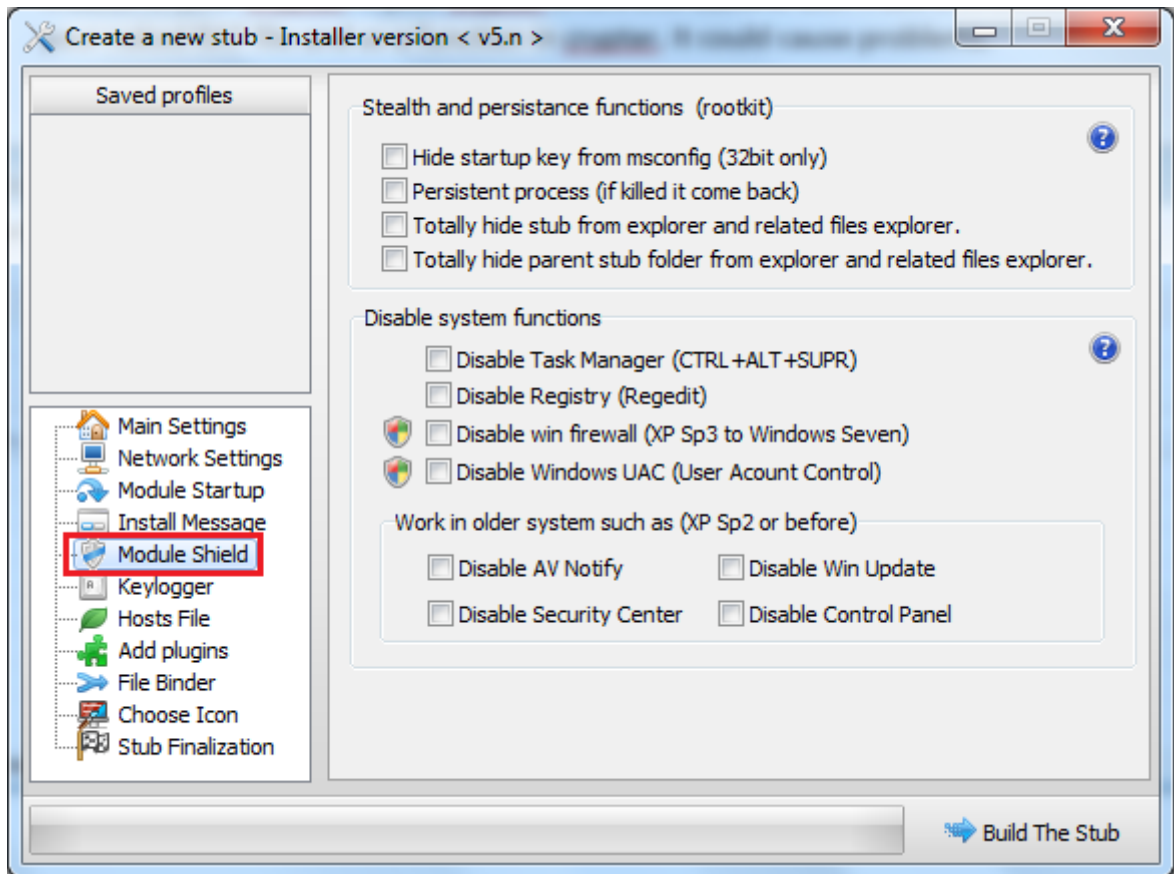
- **IP/DNS:** Enter here your DNS which you created on Noip.com for example: crack123.no-ip.biz
- **Port:** Enter here your Port, which you opened in your router/VPN and listen to in your DarkComet RAT
- **Click Add after you filled it with those informations.** You can add DNS as much as you want.



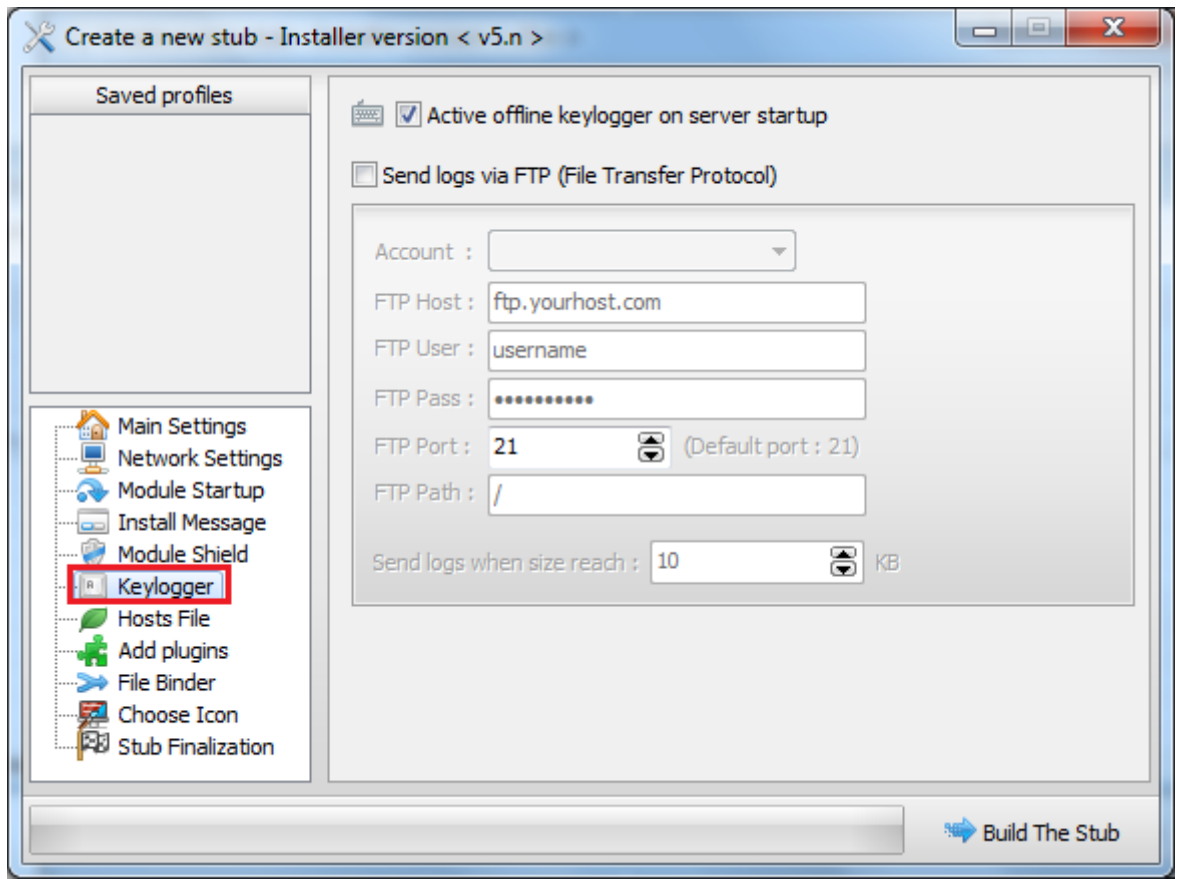
Make sure everything is deactivated in Module Startup. It would made problems if you want to use your file with a Crypter.



You can add an Install Message if you want, it will be shown directly after the slave clicked your RAT. You can use it, but I would recommend to use the Fakemessage Creator in your Crypter, if your crypter offers this feature. Don't use this feature in your naked RAT file and as a function in crypter. It could cause problems.

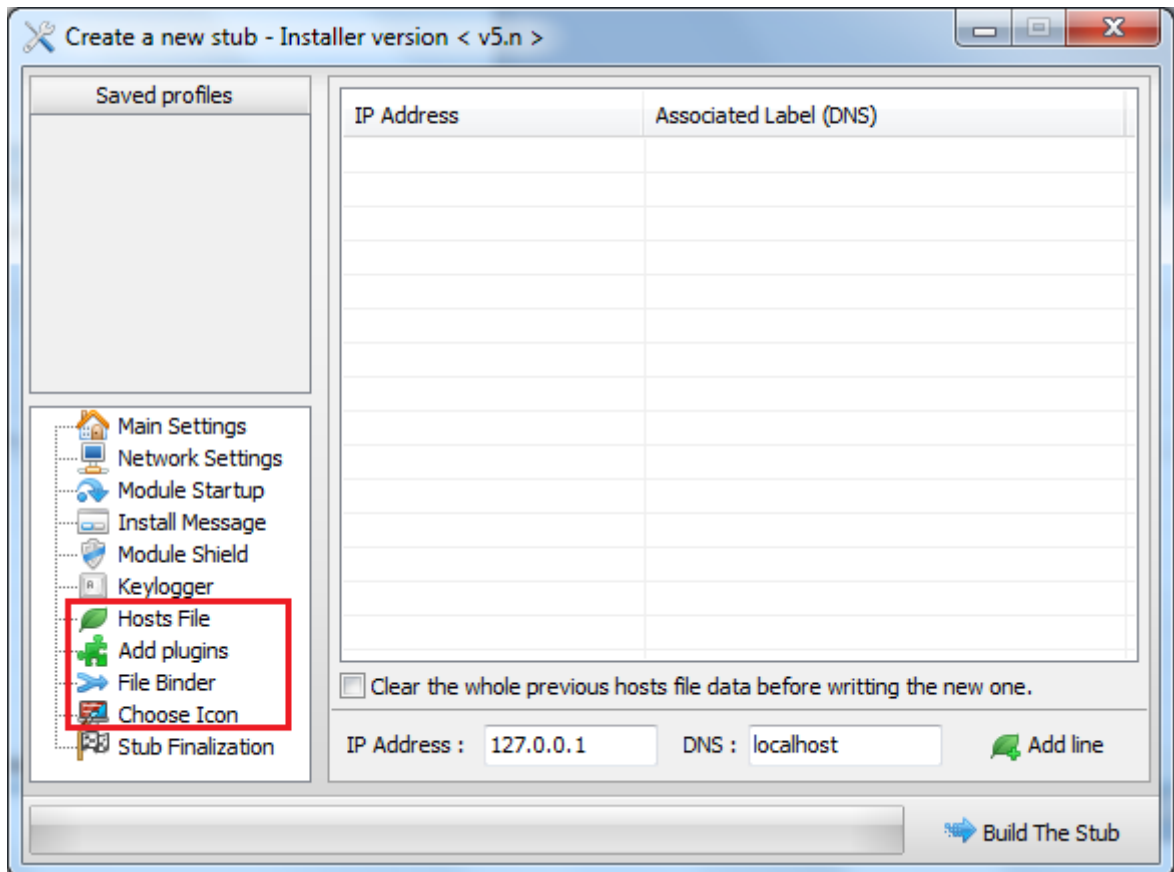


Be sure that everything is deactivated here



The keylogger is an very important feature, with a keylogger everything what your slave is writing will be saved. If you want such an feature, click on “Active offline keylogger on server startup”.

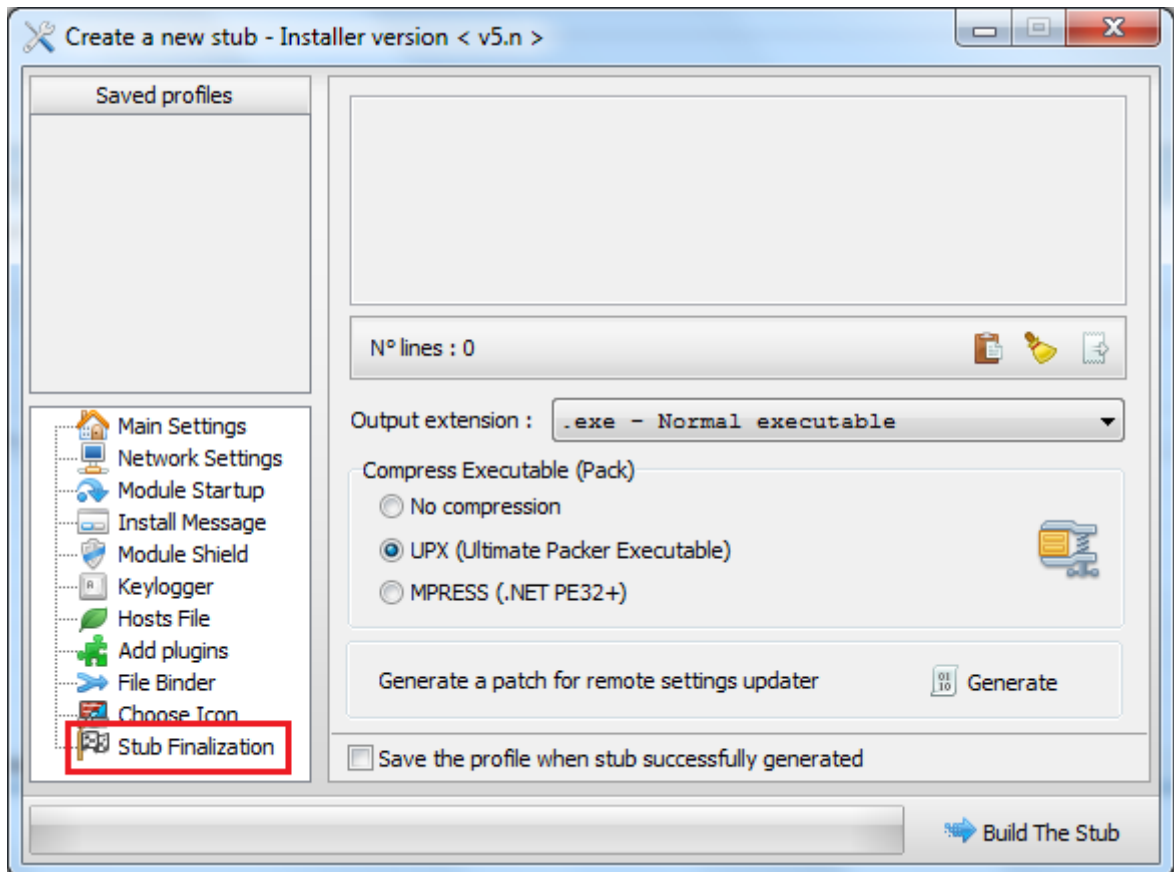
You also can send the logs to your FTP server, just fill your FTP Account data into the fields and activate it with a click on “Send logs via FTP (File Transfer Protocol)”



You can ignore the following features:

- Hosts File
- Add plugins
- File Binder
- Choose Icon

These features are not necessary for us. There are either useless or would cause problems with a crypter.



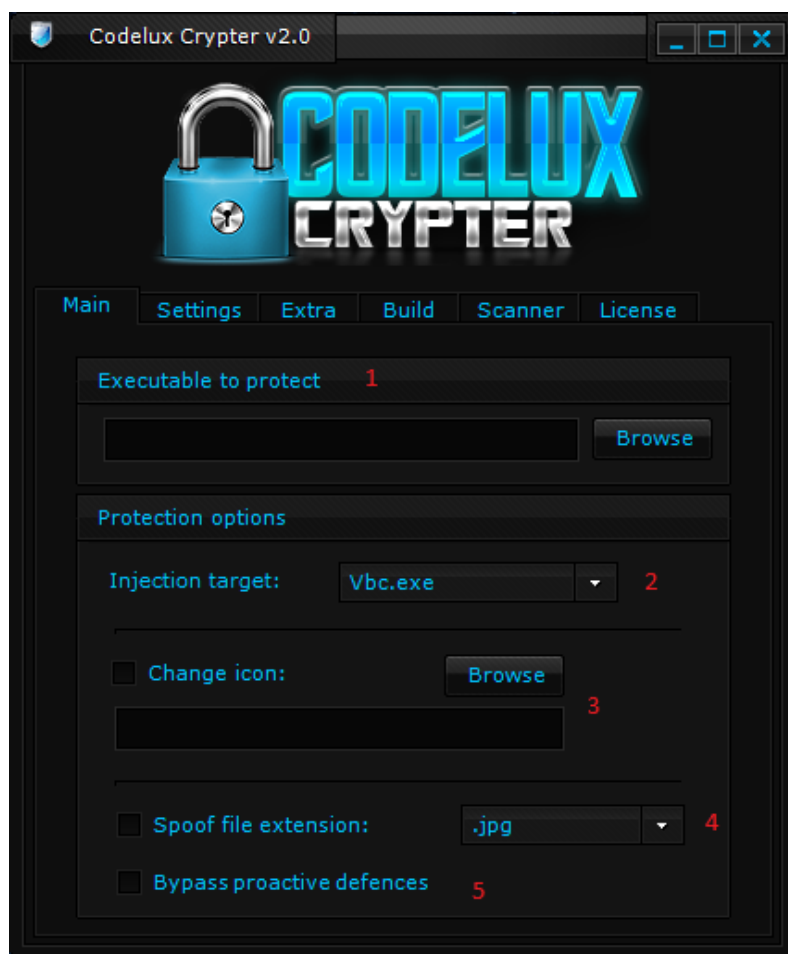
- **Output extension:** You should chose the .exe option
- **Compress Executable (Pack):** Be sure the mark is on “UPX (Ultimate Packer Executable)”
- **Save the Profile:** Make a mark on it if you want to save your setting if you want to make a naked RAT file (Stub) again.

Now click on “Build the Stub”. You now just have to choose where you want to save your file. Congratulations! You now made your first Stub (Naked RAT File).

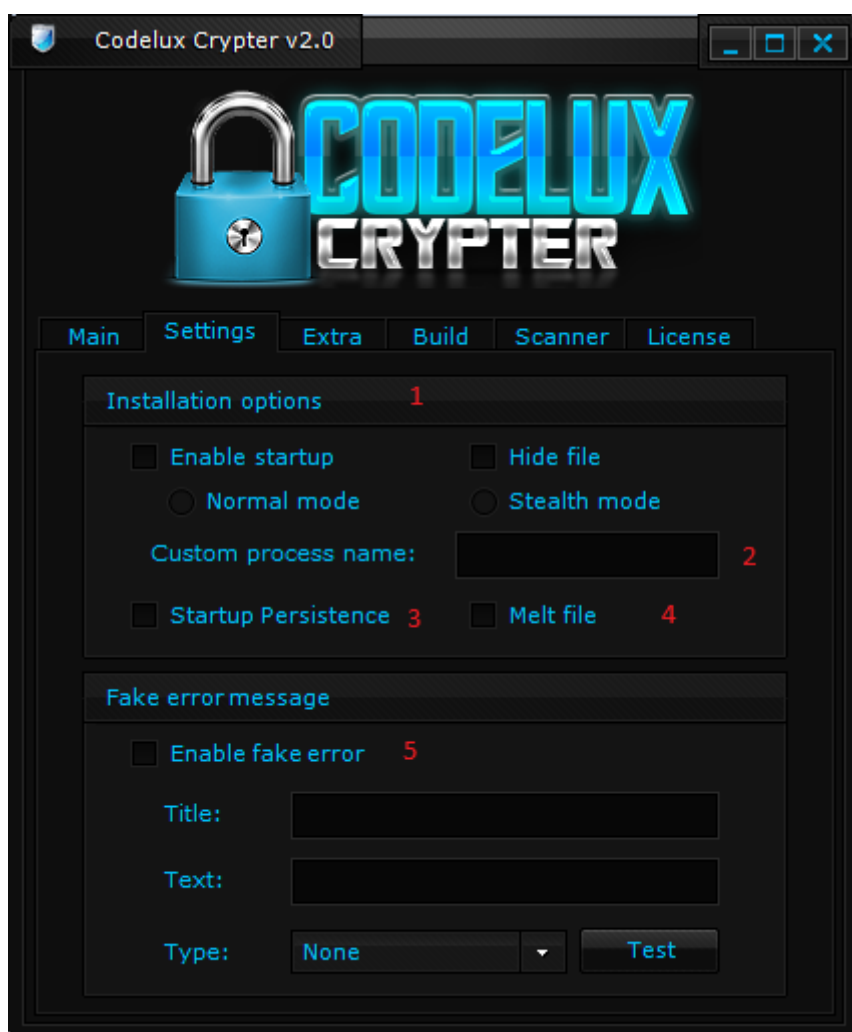
Encrypt your Stub with a Crypter

Now we need to encrypt your file so antivirus programs won't find it. Because I can't show you any good crypter on HF, I will show you one that I actually use and which is very good. It's the [Codelux Crypter](#). Thanks again to [Delirium™](#), who gave me a bunch of screenshots of his crypter even my license expired right when I wanted to make this guide. All crypters are very similar so I can explain it good for you with this one.

I will now explain what every single window or feature means to you and I will explain which features you should use. At the end you have to decide your own features, I will just give you an advice.



1. Here you put your "Naked RAT" (Stub) File into it, just click "Browse" and search it.
2. Here you are choosing which Injection method should be used (I prefer Vbc.exe)
3. After encrypting your file, you can choose a new look for your file. So if you want that your file should look like a picture, then you should use a .jpg icon. Here you can find some icons: <http://findicons.com>
4. You can spooof your file into a .jpg file. But be carefull because it will look like this: **mystub.exe.jpg**
5. It's a one minute delay. That means, after your victim clicked your file, it will execute after one minute. I recommend to use this because this will bypass antivirus features like SONAR. It's possible that other crypters are giving you the choice to make different execution delay times.



1. It's highly recommend that you use this one. After the execution, the crypter will make an installation to folders like %appdata or %temp. It also will add your file to an autostart. Just click "Enable Startup" and choose "Stealth mode". I not recommend to use "Hide file" and "Normal mode".
2. In the "Custom process name" you can decide how your file should look in the Task manager, take something like "Adobe Update", something that doesn't look so suspicious.
3. If activated, it will automatically open again after your slave closed the process/file.
4. If activated, your file will be melted or destroyed after execution.
5. Here you can implement a fake error message. If you didn't already made one in your Stub, you can choose one here. ATTENTION: Don't use this feature if you already made a fake message in your Stub.



1. Here you can bind your Stub with another file. For example, if you want to spread with the Torrent/Crack method, you can just easily bind your file with an existing exe of the crack.
2. If activated, you can decide if your stub should download a file right after execution.



1. You can make a one Assembly information or clone one! You should use this feature because it makes your file more unsuspecting for antivirus programs.
2. Click here to start the encryption. After that, you made your first own Trojan, hurray!

Advertisement



**Get Tons Of
FEMALE SALVES
Now!!**

- ✔ HOT FEMALESLAVES FAST!
- ✔ ALMOST JUST COPY&PASTE
- ✔ TIPS AND TRICKS
- ✔ INSTANT SETUP

CLICK HERE

Test your File

Now we have it! We made a FUD file which you can spread now. But wait, before you really start to spread you should test your file before it's get out.

Sandboxie

At first, we test the functionality of our stub. You can easily do that with sandboxie.

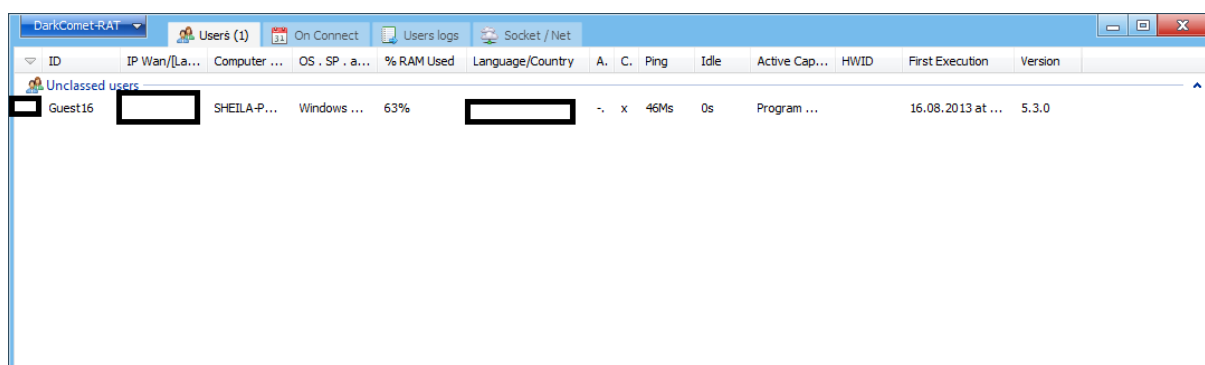
Sandboxie download: <http://www.sandboxie.com/index.php?DownloadSandboxie>

Install the program and start it.

After you started you started the program, right click your file and choose "Execute in Sandboxie"

After that you will see the file in sandboxie. After a while a process should start called "VBC.exe" (Or any other injection, that depends which injection you choose in your encryption)

If you made everything right, you should appear in your RAT program.



Elementscanner

If your crypter doesn't have an integrated virus scanner, you can test it on elementscanner.com. I highly recommend just to test it on this site! The most virus scanner sites distribute your file, which makes your file detected and also useless.

If its look like this, it's Fully Undetectable

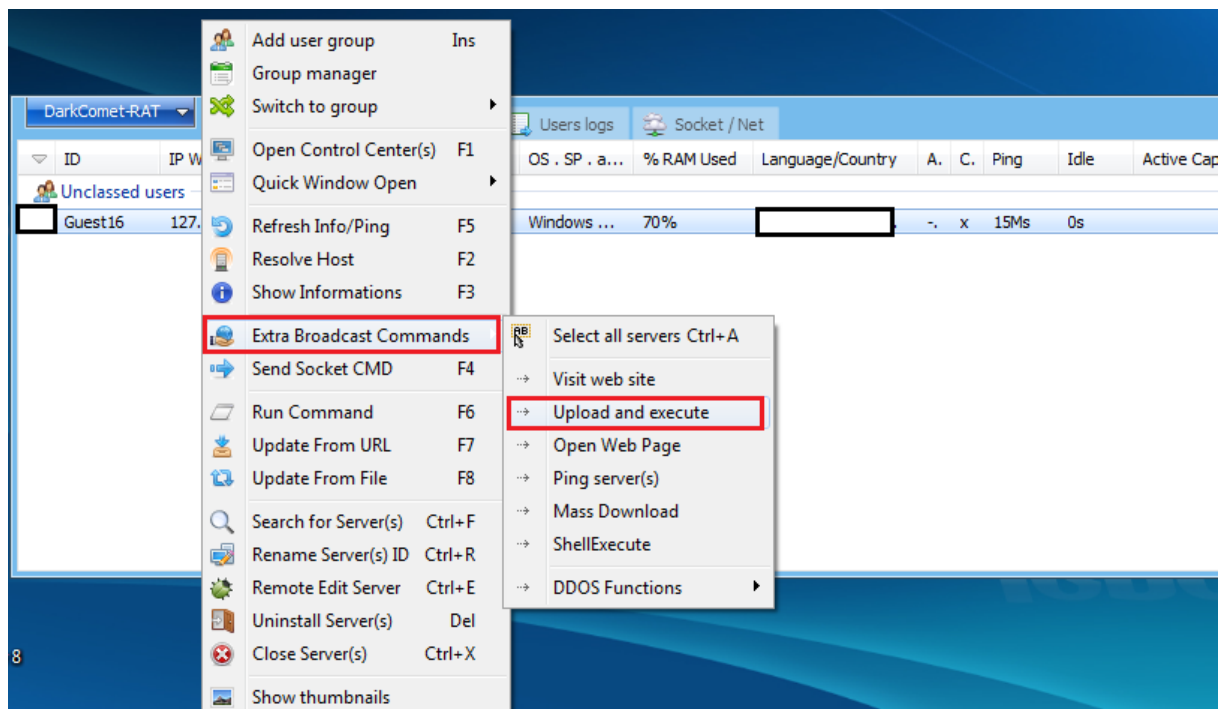


The Slave test

You also can test the functionality of your file with a simple slave test.

The only requirement is that you must already have a slave and be sure you test it on a slave which don't have already file with the same Mutex like your file (See: Make a naked RAT file).

Just click with a right click on the slave -> Extra Broadcast Commands -> Upload and Execute. Now you just have to choose your file which you want to test. When the slave is arriving again, the file works!



Cammy

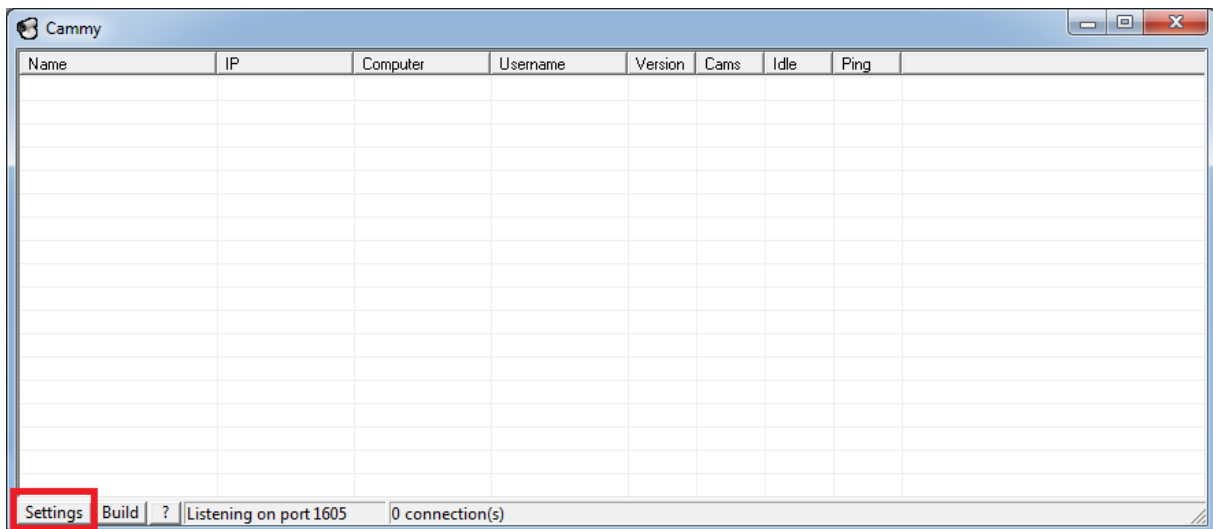
Now I want to tell you some things about Cammy. Cammy is actually an open source project. You can download it at the forum of ic0d or with my direct link.

Cammy Download: Thread link: <http://www.ic0de.org/showthread.php?9205-Cammy-2-0>
(You have to register)

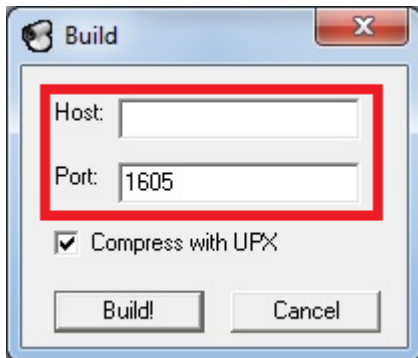
Direct Download: <http://ge.tt/9DFCJ2p/v/0>

Cammy is very very unstable when you start it with many slaves. It's almost impossible to start it when you have more than 10 slaves online. But there is a trick that I want to show you, but before I want to show you how you make a stub and configure it.

1. Start Cammy.exe
2. Click on "Settings"



5. As you can see, it's similar to DarkComet. Just enter a DNS in the "Host" box and the port you are listening to. Be sure "Compress with UPX" is marked. Then click on "Build!".



6. Now you have to encrypt the Stub (See: Encrypt your Stub with a crypter)
7. Execute it via the "Upload&Execute" DarkComet feature on your slaves computer.